HERRAMIENTA SOFTWARE PARA MEDICIÓN DE DESEMPEÑO DE SERVICIOS SOBRE UNA INFRAESTRUCTURA TI PARA LA EMPRESA KEYNETTIC S.A.S.

Fabián Mañunga Camacho

Director: Ing. Oscar J. Calderón C.
Asesor: Ing. Mauricio Gómez Sevilla

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo I+D Nuevas Tecnologías en Telecomunicaciones (GNTT)
Universidad del Cauca
Popayán – Cauca
2021

HERRAMIENTA SOFTWARE PARA MEDICIÓN DE DESEMPEÑO DE SERVICIOS SOBRE UNA INFRAESTRUCTURA TI PARA LA EMPRESA KEYNETTIC S.A.S.

Universidad del Cauca

Trabajo de grado en Modalidad Práctica Profesional
Presentado como requisito para optar el título de Ingeniero en Electrónica y Telecomunicaciones

Fabián Mañunga Camacho

Director: Ing. Oscar J. Calderón C.
Asesor: Ing. Mauricio Gómez Sevilla

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo I+D Nuevas Tecnologías en Telecomunicaciones (GNTT)
Universidad del Cauca
Popayán – Cauca
2021

Contenido

Lista de Figuras

Lista de tablas

Lista de acrónimos

API	*Application Programming Interface*, Interfaz de Programación de Aplicaciones
AWS	*Amazon Web Services,* Servicios Web de Amazon
CCTV	*Close Circuit Television, Circuito Cerrado de Televisión*
DHCP	*Dynamic Host Configuration Protocol,* Protocolo de Configuración Dinámica de Host
DNS	*Domain Name System,* Sistema de Nombres de Dominio
FTP	*File Transfer Protocol Protocol,* Protocolo de transferencia de archivos
GLPI	*Gestionnaire Libre de Parc Informatique*, Gestión de Servicios de Información
HTTP	*Hypertext Transfer Protocol,* Protocolo de Transferencia de Hipertexto
HTTPS	*Hypertext Transfer Protocol Secure,* Protocolo Seguro de Transferencia de Hipertexto
ICMP	*Internet Control Message Protocol,* Protocolo de Mensajes de Control de Internet
IMAP	*Internet Message Access Protocol,* Protocolo de Acceso a Mensajes de Internet
IP	*Internet Protocol*, Protocolo de Internet
IT	*Information Technology*, Tecnología de la Información
ITIL	*Information Technology Infrastructure Library,* Biblioteca de Infraestructura de Tecnología de la Información
JSON	*JavaScript Object Notation,* Notación de Objeto de JavaScript
KPI	*Key Performance Indicator,* Indicador Clave de Desempeño
LAN	*Local Area Network,* Red de Área Local
OID	*Object Identifier,* Identificador de Objeto
PMI	*Project Management Institute,* Instituto de Gestión de Proyectos
QoS	*Quality of Service,* Calidad de Servicio
SLA	*Servive Level Agreement,* Acuerdo de Nivel de Servicio
SNMP	*Simple Network Management Protocol,* Protocolo Simple de administración de Red
SSH	*Secure Shell,* Capa Segura
TCP	*Transmission Control Protocol,* Protocolo de Control de Transmisión
TIC	Tecnologías de la Información y la Comunicaciones
TOGAF	*The Open Group Architecture Framework,* Marco de Arquitectura del Grupo Abierto
UDP	*User Datagram Protocol,* Protocolo de Datagrama de Usuario
VoIP	*Voice over Internet Protocol,* Voz sobre el Protocolo de Internet
WAN	*Wide Area Network,* Red de Área Amplia

DESCRIPCIÓN DEL PROBLEMA

La diversificación hacia nuevos mercados en diferentes sectores de la economía, ha generado que a nivel corporativo las empresas que los impulsan deban contar con servicios e infraestructuras de comunicaciones modernas y confiables, que les permitan satisfacer las necesidades de los actuales y nuevos clientes. Los servicios que buscan y proveen las empresas deben ser eficientes, estables y escalables, de tal forma que les permitan operar apropiadamente y generar un crecimiento organizado [1].

En este contexto, hay diferentes organizaciones en países latinoamericanos y a nivel nacional que reflejan un alto índice de crecimiento empresarial, como resultado del fenómeno de la globalización en la actividad económica, social y de desarrollo tecnológico [2]. En Colombia, por ejemplo, las empresas y los usuarios en general reflejan un crecimiento permanente en la demanda de prestación de servicios de comunicaciones, en el caso particular de los usuarios, se presentó un incremento en el acceso a redes de datos, conexiones a Internet y de telefonía móvil, según MinTIC en el primer trimestre del año 2020 se registró un aumento de 161 mil conexiones a Internet fijo frente al último trimestre del año anterior, además las conexiones de dispositivos móviles a Internet cerraron en ese mismo periodo de tiempo con una cifra cercana a los 30 millones de accesos en Colombia [3].

En Colombia según lo analizado por el ministerio de Tecnologías de la Información y las Comunicaciones en su estrategia integral para mejorar la prestación de los servicios fijos y móviles del país, encontró que, en 2019, los usuarios presentaron quejas por calidad del servicio debido a llamadas caídas, intermitencia, error de facturación y no disponibilidad del mismo [4]**,** todo ello, contrario a los objetivos propuestos por el MinTIC, en los cuales se reconoce la importancia de las Tecnologías de la Información y las Comunicaciones (TIC) para el desarrollo social y económico del país, pues tiene impactos positivos en la productividad, innovación y el acceso a la información, lo cual se traduce en crecimiento económico de largo plazo, reducción de la desigualdad y, por ende, mejoras en la calidad de vida [5].

Acorde a lo anterior, se hace importante para los proveedores de servicios de TI, realizar un diagnóstico de cuál o cuáles son los problemas que efectivamente los están afectando y de esta manera mejorar la percepción del servicio que reciben los usuarios.

En la ciudad de Bogotá, se encuentra la empresa de consultoría KEYNETTIC S.A.S, creada por ingenieros egresados de la Universidad del Cauca, con el propósito de prestar servicios de consultoría a las empresas de telecomunicaciones (TELCOS) y grandes compañías del sector, en el uso, implementación y monitoreo de tecnología en los procesos productivos.

En el portafolio de servicios de la empresa KEYNETTIC S.A.S, el tipo de consultoría que brinda se apoya en la experiencia de sus ingenieros y en el uso de los principales marcos de referencia y metodologías reconocidas por la industria de las telecomunicaciones y de la gestión TI, tales como la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL, *Information Technology Infrastructure Library),* el Marco de Arquitectura del Grupo Abierto (TOGAF, *The Open Group Architecture Framework),* buenas prácticas para trabajar

colaborativamente *(SCRUM)* y los documentos del Instituto de Gestión de Proyectos (PMI, *Project Management Institute)*.

Por lo anterior la empresa KEYNETTIC S.A.S, en su experiencia como consultora, percibe la necesidad de contar con una herramienta adaptada, que le permitiera analizar el desempeño de los servicios que usa un cliente corporativo, los cuales son suministrados por un gran proveedor de servicios TI (un tercero), con el ánimo de verificar y contrastar reportes de desempeño y métricas de los servicios prestados que son entregados por el proveedor.

Esta situación se presenta debido a que el proveedor entrega reportes a la empresa cliente, pero estos no satisfacen sus expectativas, ya que no tienen forma de contrastar la información suministrada. La percepción del cliente es diferente respecto al servicio usado y, por lo tanto, requiere de una fuente alterna que indique los valores de las métricas de desempeño de los servicios que recibe de su proveedor.

Debido a lo mencionado anteriormente, la empresa KEYNETTIC S.A.S. necesita que la herramienta *Elastic Stack* se adapte a unos requerimientos de monitoreo de desempeño de servicios de Tecnologías de la Información (TI) que se encuentran en operación, y así identificar las brechas o problemas presentes en la prestación de los servicios.

La empresa KEYNETTIC S.A.S. selecciona la herramienta mencionada debido a que tiene utilidades de *Machine Learning*, y a que facilita la captura, análisis y correlación de eventos que ayudan a realizar un diagnóstico en cuanto a uso y capacidad de los servicios prestados. De esta manera, como empresa consultora, dispondrá de una herramienta adaptada que le facilite la implementación de estrategias que permitan mejorar las condiciones de la prestación del servicio a los clientes en términos de calidad y eficacia.

1. CAPÍTULO I. SERVICIOS TI

1.1 Descripción de Servicios TI

Un servicio es una unión de recursos que se suministran a los usuarios para que logren sus objetivos de negocio; por medio de estos recursos se puede solucionar problemas, mejorar las condiciones económicas y obtener un crecimiento empresarial. Los servicios deben ser robustos, confiables y de calidad para el cliente [6].

Las Tecnologías de la Información aluden a las capacidades tecnológicas y de sistemas de información que pueden usar y desarrollar las empresas para integrar e implementar en sus organizaciones, cumpliendo con la misión, visión y objetivos de las mismas. Por otro lado, se define a las Tecnologías de la Información y Comunicación como un grupo de elementos conformado por técnicas y herramientas que se usan para la captura, procesamiento, almacenamiento y envío de información con el objetivo de analizarlos para que ayuden en la solución de fallos y problemas [7].

En el entorno globalizado en el que se está, es necesario para toda organización fortalecer las estrategias de implementación, desarrollo de las tecnologías de información y las comunicaciones con el fin de optimizar, robustecer cada uno de los procesos que soportan, como respuesta al entorno dinámico para mejorar los procesos de trabajo, las estrategias de negocio que se traducen en rendimiento, competitividad, y mejor atención a los clientes o usuarios [8].

Las empresas u organizaciones han comenzado a invertir y explorar soluciones que hagan uso de las TI con el objetivo de tener ventajas competitivas y mejorar sus procesos productivos. El sector de TI ha mostrado un desarrollo y crecimiento rápido, debido a esto se ha generado la necesidad de incorporar tecnologías de información a los procesos del negocio, a su vez ha creado un nuevo mercado de empresas consultoras que proveen servicios [9], soluciones de TI, incrementando significativamente el uso de sus servicios en el medio, para llevar a cabo las actualizaciones de infraestructura y reducción de fallos [10], aprovechando al máximo la infraestructura TI que se tiene a disposición o se implemente, obteniendo una mejora significativa en el funcionamiento de los servicios de la empresa.

Los servicios de TI son servicios que hacen uso y necesitan de tecnologías de información para su funcionamiento, estos servicios pueden ser prestados a clientes externos o usados por las empresas internamente para el trabajo en sus actividades de negocio. El autor O. Meneses en el catálogo de servicios versión 1.0 expresa que un servicio de TI es un “conjunto de capacidades tecnológicas y/o profesionales que por sus características son percibidas por el usuario como un todo que soporta su actividad de negocio” [11]. Los servicios TI se pueden agrupar como servicios tecnológicos y servicios profesionales, según sea el aporte de valor al usuario y su afinidad tecnológica de los elementos y sistemas respectivamente [11].

- **Servicios Tecnológicos**: Estos servicios usan capacidades técnicas que tienen elementos, equipos y sistemas tecnológicos.

- **Servicios Profesionales:** Este tipo de servicios lo conforman actividades de valor añadido que brinda el equipo de personas de TI, para garantizar la prestación del servicio y su gestión.

Debido a las necesidades de nuevos y mejores servicios, y a la gran cantidad de usuarios de los mismos, hoy en día existen una gran variedad de servicios de TI enfocados en solucionar los problemas y requerimientos de los clientes, sean estos corporativos o residenciales. A continuación, se presentan algunos de los servicios TI más usados hoy en día.

1.1.1 Navegación Web

El servicio web permitir la interoperabilidad entre máquinas a través de una red de datos [12], por medio de una aplicación o sistema software al que se puede acceder mediante protocolos HTTP (*Hypertext Transfer Protocol*) o HTTPS (*Hypertext Transfer Protocol Secure*).

Dentro de las razones para utilizar servidores web se destaca que permiten integrar diferentes aplicaciones, independientemente de sus propiedades o de las plataformas sobre las que se instalen. De tal manera, es posible que servicios y software de diferentes compañías en diferentes lugares del mundo puedan ser fácilmente combinados para proveer servicios integrados [13]. Los servicios web son muy utilizados por las empresas, ya que incluyen el uso del correo electrónico a través de la Web, descarga de archivos (texto, imagen, audio, vídeo, e-books), descarga de programas, aplicaciones, chats, videoconferencia a través de la Web, publicación, consulta de blogs, respuesta a formularios en línea para diferentes suscripciones o reservas, consultas, gestiones administrativas, subastas, compras en línea, entre otras [14]. A continuación, se presentan algunas ventajas y desventajas según E. López [15].

Ventajas

- Permite acceder a múltiples contenidos (información infantil, multimedia, imagen).
- Brinda la posibilidad de difusión de contenidos propios.
- Permite la masificación del conocimiento, por ejemplo: investigaciones, nuevas tecnologías desarrolladas, etc.
- Permite la interacción con grupos de interés a largas distancias.
- Brinda espacios para la generación de nuevos empleos en cualquier parte del mundo.
- Ofrecer a las personas acceso a nuevos formatos de entretenimiento.

Desventajas

- Los metadatos de las personas se usan por terceros con fines desconocidos.
- Es generador de sedentarismo en las personas.
- Existe riesgo de ciberdelincuencia por ejemplo robo de dinero e información a empresas, suplantación de personas, entre otros.
- Acoso en línea (Bullying) a las personas (niños, adolescentes).
- Algunos sitios web tienen publicidad invasiva dentro de su contenido.

- Se puede encontrar noticias falsas, ya que alguna página web no tiene control de lo que se publica en ellas; este tipo de información crea caos y desinformación en las personas que acceden a estos sitios web.

1.1.2 VoIP (*Voice over IP*)

El autor L. Boza, en [16], presentó el Diseño e implementación del plan piloto de un sistema de comunicación VoIP usando tecnologías de código abierto, y C. Gauloto en [17], describe la Implementación del servicio de VoIP para los laboratorios de computación de la FICA, en dichos trabajos exponen la Voz sobre IP (VoIP, *Voice over IP*) como una tecnología emergente, que permite enviar comunicaciones de voz y video entre un origen y un destino por medio del Protocolo Internet.
Las señales de voz que ingresan a la red, se convierten en paquetes IP que viajan por una Red de Área Local (LAN, *Local Area Network*) o una Red de Área Amplia (WAN, *Wide Area Network*), este proceso de envió de información se hace regularmente sobre tecnologías Ethernet [17]. Algunos servicios que ofrece VoIP son: desvío de llamadas, llamada en espera, grabar llamada, operadora automática, informes de llamada, identificador de llamada, repetir llamada. M. Vinueza en Estudio detallado del uso RTP/RTCP y Servicios de QoS y QoE en Internet para la VoIP [18], mencionan algunas ventajas y destajas que se muestran a continuación.

Ventajas

- Ofrece una alta escalabilidad ya que los elementos que la componen o se necesitan para que funcione el servicio son computadores, teléfonos, servidores y softphones, los cuales en el mercado son de fácil adquisición y a costos bajos; por lo tanto, se puede ampliar la cantidad de usuarios de manera rápida y con baja inversión.
- Brinda la posibilidad de usar la infraestructura ya existente, facilitando de esta manera la implementación, instalación y mantenimiento.
- Brinda portabilidad al permitir recibir y realizar las llamadas desde cualquier lugar del mundo en el cual haya una conexión a internet y se pueda acceder al proveedor de la cuenta de teléfono.

Desventajas

- En ocasiones la elevada presencia de variaciones del retardo en la red LAN o la WAN por la saturación en la red, pueden generan que las llamadas sean rechazadas.
- Puede tener fallos y dejar fuera de funcionamiento el servidor VoIP, cuando hay virus en el servidor.
- Puede ser objeto de fraudes de suplantación y vulnerable a ciberataques sino se configura adecuadamente su protección.

1.1.3 eCommerce

J. Gonzales en Marketing y Ecommerce [19], define e-Commerce como “marketing y venta de productos o servicios a través de Internet”, también conocido como comercio electrónico. Este servicio permite el intercambio de productos y servicios haciendo uso de

computadoras, tabletas o smartphone por medio de internet [20], tiene una gran demanda ya que muchos productos y servicios como libros, dispositivos electrónicos, software, música, casa, carros, compra tiquetes de avión, entre otros, se pueden adquirir por este medio, debido a esto se le considera como una tecnología muy disruptiva [21].

Ventajas

- Permite a los usuarios una mayor comodidad para hacer compras y adquisición de productos desde sus hogares.
- Existe una gran variedad de productos y servicios para que los usuarios los adquieran, casi cualquier cosa se puede comprar por ejemplo ropa, comida, electrodomésticos, medicinas, planes de viajes, etc.
- Otorga una reducción de costos a los dueños de las tiendas virtuales, ya que no deben pagar arriendo por el local, se puede abrir más rápido que una tienda física pues no hay que construir espacios físicos, solo se necesita infraestructura y conectividad a internet para crear el sitio y comenzar a vender producto y servicios.
- Ofrece a los usuarios, la facilidad de adquirir productos y servicios las 24 horas de los 7 días de la semana, ya que la tienda online no cierra, como por el contrario lo hace una tienda física, la cual ofrece servicios solo en las horas laborales.

Desventajas

- Puede presentarse congestión en el sistema que soporta la realización de compras debido al alto volumen de clientes que están solicitando producto, o pueden caerse el servicio durante la realización de la compra de un producto o servicio lo cual genera una mala calidad de la experiencia.
- Desconfianza y miedo por parte de los compradores ya que pueden ser víctimas de robo, suplantación de algunos sitios de tiendas en líneas o también perder el dinero de la compra debido a que el vendedor no entrega los productos en las condiciones que lo ofrece en la tienda.
- Problema con los envíos por parte del vendedor al cliente, algunos tiempos de envíos pueden tardar debido a que el vendedor no tiene inventario o la ubicación del vendedor se encuentre muy retirada de la su cliente.

1.2 Problemas presentes en las redes

Los servicios TI que soportan las redes de comunicaciones son cada vez más robustos, y crecen de manera continua. Las infraestructuras de comunicaciones tienen recursos limitados, que deben operar de la manera más eficiente posible. Algunos factores, presentes en estas infraestructuras y que deben ser considerados para una correcta prestación de servicios son los retardos y la perdida de información que tienden a producir errores.

1.2.1 Retardo

Retardo es el tiempo que demora en llegar un paquete desde su origen a su destino [16]. En algunos casos se asocia a las líneas y tecnologías de transmisión usadas. Dentro de los

tipos de retardo se pueden encontrar retardo de procesamiento, retardo de buffering y retardo transmisión.

- **Retardo de procesamiento:** es el tiempo se usa para analizar la información contenida en la cabecera de un paquete y decidir sobre cual interfaz de salida enviarla, por ejemplo, en un enrutador el retardo de procesamiento es el tiempo que este invierte en determinar la ruta hacia donde se dirige el paquete.
- **Retardo de buffering**: es el tiempo que espera un paquete, regularmente en un buffer, hasta que se le transmite, en algunos casos se asocia a los sistemas de encolado que tienen los dispositivos de red.
- **Retardo de transmisión:** Es el tiempo que se requiere para colocar todos los bits en un paquete al medio de transmisión.

1.2.2 Jitter o variación retardo

En Diseño e implementación del plan piloto de un sistema de comunicación VoIP usando tecnologías de código abierto realizado por L. Boza [16], el Jitter se define como “la variación en el tiempo en la llegada de los paquetes consecutivos”, los cuales pueden ser generados por la congestión en la red por la cantidad de tráfico cursado por ella, perdida de sincronización, entre otros.

1.2.3 Latencia

La latencia se puede definir como “el tiempo que demora un paquete en trasmitirse dentro de una red” [22]. La latencia se le conoce como retardo total.

1.2.4 Congestión

La congestión es un fenómeno que se produce por múltiples razones, entre ellas, cuando una interfaz de un dispositivo de red recibe más tráfico de aquel que es capaz de procesar [22], cuando las capacidades de los enlaces han sido pobremente dimensionados, cuando existen demasiados usuarios generando tráfico de red, etc. Todo ello contribuye a la generación de retardos.

1.2.5 Perdida de paquetes (*Loss*)

Con este parámetro se identifica la no llegada de los paquetes enviados al destino [23]. Se presentan cuando los paquetes que viajan por la red llegan a puntos de saturación en las interfaces (encolado) y se descartan por falta de capacidad de almacenamiento, a daños en los enlaces, o problemas de enrutamiento [24].

1.3 Medición, Métricas, KPI, Logs

1.3.1 Medición

Se define como un medio para reducir la incertidumbre apoyada en observaciones que se expresan en unidades cuantificables [25]; el objetivo principal es lograr que las descripciones de las métricas aporten datos significativos, siendo objetivas, exactas y seguras [26]. La medición cuenta con una característica importante que le permite establecer valores numéricos, para proporcionar una respuesta definitiva y real, de esta manera se tiene una apreciación de si los valores favorecen o empeoran las cosas que se están estudiando o analizando [25].

La medición suministra información clave para las empresas que hacen uso de tecnologías de la información ya que ayudan a evaluar, predecir, mejorar los servicios y recursos que tienen en uso. A continuación, se presenta las razones de por qué es importante medir.

- **Evaluar:** con los valores obtenidos de la medición se analiza el desempeño y rendimiento de los sistemas de red y servicios TI; estos proporcionan información que se puede usar para tomar decisiones, señalando problemas acerca del estado actual de los servicios voz, datos, video, entre otros que usan o se suministran a los usuarios.
- **Predecir:** con los datos recolectados de la medición se crean historiales de datos, a partir de ellos se estudian los comportamientos, fallas y errores en los servicios de TI e infraestructura que los soportan, con este estudio se llevan a cabo proyecciones para mejorar los servicios de TI.
- **Mejorar:** Las mediciones ayudan a visualizar el funcionamiento de los servicios de TI, mediante esta observación se pueden encontrar tendencias negativas y/o positivas de los valores recopilados, además con esta información se mejora el funcionamiento, rendimiento de los sistemas y servicios para que generen los resultados de los objetivos planeados por las empresas y organizaciones.

1.3.2 Métricas

Las métricas son una medición o cálculo que describen un objeto, elemento, sistema, etc., estas contienen datos sobre una variable que se requiere conocer, se expresan en unidades o porcentajes usándose para informar, gestionar, supervisar y mejorar. Las métricas de servicios TI se necesitan para medir y validar el éxito de los servicios que prestan o reciben las empresas, se utilizan en los servicios (VoIP, video, datos, base de datos, etc.), equipos de red y/o elementos de infraestructura TI. Se pueden encontrar varios tipos de métricas como, por ejemplo: métricas de eficacia, eficiencia, productividad, monitoreo, desempeño [25].

- **Métricas de eficacia:** estas métricas indican el grado en que una actividad cumple su propósito y logra los objetivos. Son importantes herramientas de gestión que proveen un valor de referencia a partir del cual se puede establecer una comparación entre las metas planeadas y el desempeño logrado.
- **Métricas de eficiencia:** estas métricas especifican como una organización o empresa hace uso de los recursos para realizar actividades administrando

productos y servicios, aportan a las empresas información importante para optimizar los recursos económicos, definiendo mejoras y formas para escalar los servicios de TI [27].

- **Métricas de productividad:** este tipo de métricas describen la cantidad de trabajo que se realiza y los resultados obtenidos; describen el rendimiento que da una práctica o actividad. Para el sector de TI, la productividad se asocia con lo económico [28], por este motivo son de gran importancia, se necesitan capturar, analizar durante largos periodos de tiempo para aprender y generar información que ayude a tomar decisiones de negocios más acertadas a las empresas, esta labor debe ser constante y continua.
- **Métricas de monitoreo:** son la recolección de entradas de información numérica que se agrupan cronológicamente en listas consecutivas. Cada entrada de información contiene el valor registrado medido, marca de tiempo (*Timestamp*) cuando se registró la medición. La recolección de las métricas debe ser fácil, y de ser posible, automatizada a través de herramientas adecuadas [29].
- **Métricas de desempeño:** son medidas compuestas de indicadores, que son de suma importancia para el éxito presente y futuro de las organizaciones [30]. La información que se obtiene a través de las métricas de desempeño de los dispositivos de red y los servicios de TI, brindan un valor estratégico a las organizaciones, pues permite que, a través de estas, su análisis e interpretación se tomen decisiones de operación.

1.3.3 Indicador clave de desempeño (KPI, *Key Performance Indicator*)

Un Indicador Clave de Desempeño – KPI, es una o un conjunto de métricas que se centran en determinar y evaluar el desempeño de objetos, proyectos, empresas, etc., por medio de la verificación de los objetivos de desempeño que se han fijado con anterioridad [31]; permiten reconocer el rendimiento de una estrategia. Por medio de los KPI se define la condición del estado de un servicio, objeto, u organización en términos de bueno o malo, éxito o fracaso, aceptable o inaceptable.
Para las empresas u organizaciones es de mucho interés confrontar los resultados que arrojan las mediciones de las métricas de los servicios de TI con los objetivos previamente establecidos [32], ya que les brinda datos muy importantes para revisar si los proyectos se están ejecutando bien o por el contrario hay problemas de ejecución que implique tomar decisiones a tiempo para convertir el proyecto en exitoso.

- **Indicador:** es una métrica que se utiliza para evaluar y/o administrar algo.
- **Desempeño:** es una medición de lo que logra y/o entrega un producto, persona, servicio, equipo, entre otros.

Las métricas se convierten en KPI cuando son cruciales o de mucha importancia para evaluar el estado de un sistema, objeto, o servicios. Los indicadores se vuelven claves cuando identifican factores que afectan considerablemente a los servicios, proyectos, o empresas.

Por último, una métrica solamente se puede utilizar como KPI si tiene un valor objetivo definido y una tolerancia (capacidad o nivel máximo que tiene para soportar un sistema o

servicio, antes de presentar fallos o inconvenientes de funcionamiento) [25]. Para poder usar métricas como KPI hay que tener en cuenta lo siguiente:

- Identificar métricas claves.
- Definir valores y tendencias objetivo.
- Definir tolerancias.

Los KPI son SMART y tienen cualidades [31] que se busca cumplan al ser definidos. Estas son:

S: Specific (Específico): un KPI debe ser claro y enfocado en el objetivo que se desea medir.

M: Measurable (Medible): un KPI se debe poder expresar en términos numéricos.

A: Achievable (Realizable): los objetivos de un KPI deben ser razonables y realizables.

R: Relevant (Relevante): un KPI es directamente relativo al trabajo realizado en el proyecto.

T: Timely (Temporal): un KPI debe permitir su monitoreo dado en un período de tiempo acotado.

1.3.4 Logs

Los logs, a nivel práctico, son registros de eventos que se generan en dispositivos hardware o dentro de un software; son archivos de texto que sirven para encontrar vulnerabilidades, errores, debilidades, violaciones de seguridad, ataques maliciosos de virus, auditorias, manipulación de datos, entre otras [33]. Cuando se genera un log este contiene una marca temporal, denominada "*timestamp*", en la cual se indica la hora y fecha en que se generó el evento [29]. Los log tienen una clasificación y un nivel de severidad, como se aprecia en la Tabla 1."

Código	Severidad	Descripción
0	Emergency	El sistema no utilizable
1	Alert	Acción requerida inmediatamente
2	Critical	Condición crítica
3	Error	Condición de error
4	Warning	Condición de advertencia
5	Notice	Condición normal
6	Informational	Mensaje de información

Tabla 1. Clasificación de Logs

1.4 Monitoreo

El monitoreo, tal como lo expone M. Alpizar Santana, en [34], permite "recopilar información sobre las características y el estado de los recursos de interés"; esto ayuda a encontrar de forma más acertada la causa de un evento que se presentó, esto se lleva a cabo mediante la captura de los datos en el instante que ocurrió el evento, de esta manera se determina el estado de un sistema y así informar rápidamente para tomar decisiones sobre el caso.
Por otro lado, F. Otarán y N. Perera [29], presenta el monitoreo como "el proceso de mantener en constante observación la existencia y magnitud de los cambios de estado y el

flujo de datos de un sistema", con la finalidad de conocer los errores, problemas y fallas de lo que se está monitoreando. Adicional se define un sistema de monitoreo al grupo de elementos software usados para la captura, adecuación, transformación y visualización de información.

Los sistemas de monitoreo convierten en información las métricas recolectadas del funcionamiento de las aplicaciones y de los sistemas en información clave para el negocio de las empresas, puesto que se recopilan datos de la experiencia de usuario, y estos al ser procesados permiten identificar si los sistemas y aplicaciones están operando correctamente como también revisar la calidad del servicio que está recibiendo el cliente final.

En el tiempo actual el mundo se ha vuelto muy competitivo en el sector de telecomunicación, telemática y servicios de TI [35], con el desarrollo de las redes de datos y redes de comunicación, la navegación por internet y las compras hechas por medio de aplicaciones , páginas web se han incrementado un 387% en el año 2020 respecto al año 2019, debido a la pandemia del covid-19 [36], esto genera un alto volumen de datos que debe ser soportado por una infraestructura de TI compleja y robusta, que contiene una numerosa cantidad de elementos de red y dispositivos TI, que de no ser controlados pueden generar problemas en la conectividad, cuellos de botella críticos en la red e indisponibilidad en los servicios.

Respecto a lo anterior, las empresas u organizaciones buscan administrar los servicios y la infraestructura de TI mediante uso del monitoreo, ya que a través de la recolección y procesamiento de información se detectan de manera temprana en menor cantidad de tiempo algunos eventos de alteración o caída de los servicios de TI; además permite identificar problemas futuros por medio de la correlación de eventos y con esta ayuda solucionar oportunamente los fallos en los servicios TI para que la afectación por indisponibilidad sea mínima.

El monitoreo y la medición son los elementos principales para realizar intervenciones y toma de decisiones durante el desarrollo de un proyecto, por ello se tiene que monitorear constantemente para recopilar datos que permitan identificar acciones y/o tendencias las cuales fortalezcan las mejoras del sistema. Es necesario centrarse en las excepciones, tendencias, ya que esta información da soporte para corroborar el éxito o fracaso de los proyectos en ejecución validando el buen o mal funcionamiento de los servicios de TI ofrecidos a los usuarios.

A continuación, se presentan algunos beneficios de usar el monitoreo en servicios TI:

- Ayuda en las organizaciones, empresas en procesos de planificación de recursos y de capacidades, por medio del consumo de elementos hardware, software y de red.
- Permite mejorar el desempeño de los servicios de TI, haciendo un uso óptimo de los recursos de la infraestructura de TI.
- Agiliza la detección de problemas, fallos en la red, infraestructura y los servicios TI.
- Mejora la planificación de adecuaciones, mantenimientos preventivos y correctivos sobre la infraestructura de TI, a través de los informes de la red de los servicios de TI.

- Obtener datos históricos de consumos de recursos de red, hardware de los servicios de TI que ayudan a reconocer la tendencia del uso normal y anormal, logrando así configurar el consumo para obtener calidad de servicio.

M. Ortiz y A. Mori mencionan y definen algunos tipos de monitoreo usados sobre servicios e infraestructura TI [37].

1.4.1 Monitoreo Activo (*Active Monitoring*)

El monitoreo activo es “el monitoreo de un elemento de configuración o de un servicio TI que utiliza de forma regular revisiones automatizadas para descubrir el estado actual” [37]. Los autores G. Junco y S. Rabelo explican que el monitoreo activo se hace insertando paquetes en la red con el fin de medir el tiempo de respuesta, en este proceso se añade tráfico en la red para medir el rendimiento de esta [38]. Este monitoreo, en redes basadas en el stack de protocolos TCP/IP, se puede hacer empleando el Protocolo de Control de Mensajes de Internet (ICMP, *Internet Control Message Protocol*), el Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*) y el Protocolo de Datagramas de Usuario (UDP, *User Datagram Protocol*); por medio ICMP se puede diagnosticar problemas y fallos en las redes, detección de retardo y perdida de paquetes; usando TCP se mide la tasa de transferencia y ofrece la capacidad de hacer un diagnóstico a nivel de aplicación, y empleando UDP ayuda a medir la perdida de paquetes en un sentido [38].

1.4.2 Monitoreo Pasivo (*Passive Monitoring*)

El monitoreo pasivo se refiere a “el monitoreo de un elemento de configuración, un servicio TI o un proceso que depende de una alerta o notificación para la identificación de su estado” [37]. En el trabajo de G. Junco y S. Rabelo indican que el monitoreo pasivo “se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red”, sin realizar ningún tipo de intervención, se está en modo “escucha” [38]. En este tipo de monitoreo no se añade tráfico a la red, contrario al monitoreo activo.

1.4.3 Monitoreo Proactivo (*Proactive Monitoring*)

El monitoreo proactivo es “el monitoreo que trata de encontrar patrones, a partir de eventos, para predecir posibles futuros fallos” [5].

1.4.4 Monitoreo Reactivo (*Reactive Monitoring*)

El monitoreo reactivo es “accionado en función a una respuesta de un evento” [37].

1.5 Herramientas para el monitoreo de red y servicios TI

Con la evolución de los servicios y las nuevas arquitecturas de red que los soportan, los sistemas encargados de administrarlos se vuelven más complejos. Frente a estas necesidades han aparecido nuevas herramientas con mayores funcionalidades, mejor organización y módulos más robustos y de propósito específico.

Las herramientas para realizar monitoreo están creadas en software o un híbrido entre software y hardware, las cuales ofrecen funcionalidades para visualizar la red de forma completa y por medio de agente capturar una amplia variedad de información sobre métricas de dispositivos de red o computadores, como por ejemplo desempeño, consumo de CPU, memoria, almacenamiento, retardos, volumen de tráfico cursado por la red, entre otros.

Por otro lado, es muy importante que estas herramientas para el monitoreo de red permitan una visión amplia y detallada de sus componentes y servicios de red a través de una interfaz de usuario intuitiva que genere reportes de los eventos que ocurren en la red; es muy importante que una herramienta para monitorear permita detectar, supervisar, analizar elementos de red y computadores en tiempo real [34].

Se han desarrollado un gran número de herramientas para el monitoreo de redes, servidores, servicios de TI entre otros [39]. Dentro de este conjunto de herramientas se pueden identificar dos tipos: herramientas para monitoreo de código abierto y herramientas para el monitoreo de índole comercial.

Las herramientas de código abierto son limitadas en funcionalidad, reportes, tiempo de uso, alertas; dentro de la limitación de funcionalidad se puede encontrar que no permita capturar cierto tipo de información o por otro lado solo permite usar funciones básicas como captura y visualización de datos, en cuanto al tiempo de uso, se puede usar por largos periodos de tiempo, instalar, reinstalar, borrar sin ningún problema, además de poder instalarla en una cantidad ilimitada de equipos. En cuanto a alertas y reportes, algunas herramientas de código abierto carecen de dicha opción.

Las herramientas de código abierto se pueden descargar de forma gratuita de la página del desarrollador, tienen una gran cantidad de foros activos en Internet, y la documentación se encuentra disponible en la página oficial, para que sea consultada por sus usuarios y publiquen dudas o apoyen los proyectos que se están desarrollando. Otro aspecto importante, es que estas herramientas facilitan que el usuario tenga acceso al código fuente, permitiendo hacer modificaciones para sus requerimientos específicos, que posteriormente podrá compartir en el foro.

Las herramientas para monitoreo de redes de tipo comercial brindan mayor capacidad en funcionalidad, permite capturar un amplio número de parámetros de red (latencia, jitter, etc.), son más robustas, permite el uso de reportes que puede ser generados en PDF, enviándolos por correo; alertas enviadas a un celular en mensajería de texto. Brindan soporte 24/7 para fallos y configuraciones, por medio de llamadas, envío de manuales y documentación al correo, el cobro de uso varia respecto a cantidad de dispositivos a instalar, cantidad de almacenamiento que se va a usar para el monitoreo de su empresa. Al contrario de la herramienta de código abierto, estas herramientas no permiten la modificación de su código, solo se descargan, instalan y funcionan; si se requiere un parámetro adicional del cual la herramienta carece, se debe instalar y configurar módulos extra con un valor adicional.

1.5.1 Características de herramientas para monitoreo red y servicios TI

En el mercado actual se pueden encontrar una gran variedad de herramientas para monitorear redes de datos, infraestructura, servicios de TI, cada una en particular tiene sus fortalezas y debilidades. Una herramienta para monitoreo de red debe poseer, entre otras, las capacidades que se describen a continuación [34]:

Capacidades	
Escalabilidad	Monitoreo compartido de recursos
Portabilidad	Usabilidad
Ser no intrusivo	Monitoreo de KPI
Monitoreo de la carga del servicio	Extensibilidad
Robustez	Asequibilidad
Multi-tenancy	Medición del uso de recursos
Interoperabilidad	Medición del uso del servicio
Monitoreo de QoS	Capacidad de ser archivado
Personalización	

Tabla 2. Capacidades de las herramientas para monitoreo de red y servicios TI

Algunas de estas capacidades se describen brevemente a continuación.

- **Escalabilidad:** la herramienta para monitoreo debe desempeñarse igual sin importar la cantidad de elementos actuales y nuevos que se incluyan en el sistema que se está monitoreando.
- **Portabilidad:** la herramienta debe trabajar en diferentes plataformas software y sistemas operativos.
- **Ser no intrusivo:** las herramientas poseen diferentes agentes para recolectar la información requerida, estos agentes tienen un consumo de recursos hardware, es de suma importancia que este consumo sea mínimo, para que no afecte las medidas de los datos de interés por el administrador de la red.
- **Robustez:** la herramienta tiene que adaptarse a los nuevos cambios y configuraciones de la red de datos y equipo ingresados y removidos a esta, funcionar de igual manera cuando se realicen actualizaciones.
- **Usabilidad:** la herramienta para monitoreo debe ser fácil de usar, permitir la instalación, configuración y mantenimiento de forma intuitiva.
- **Capacidad de ser archivado:** la herramienta para monitoreo debe tener almacenamiento de alto flujo de datos, de esta manera posibilita el análisis de la información recolectada tiempo atrás para ser usada en identificación de problemas mediante un estudio de causa raíz
- **Monitoreo de KPI:** mediante la captura de métricas se pueden establecer los KPI's, que se monitorean en tiempo real, comparando la referencia y el valor actual medido para poder analizar el desempeño de los dispositivos y/o servicios. De acuerdo a lo anterior hacer el monitoreo de KPI's es fundamental para la administración de los Acuerdos de Nivel de Servicio (SLA, *Servive Level Agreement*).
- **Monitoreo de Calidad de Servicio:** la Calidad de Servicio (QoS, *Quality of Service)* denota los niveles de rendimiento, fiabilidad y disponibilidad ofrecidos por una aplicación y por la plataforma o infraestructura que la aloja. El monitoreo de QoS es

fundamental para los usuarios que esperan que los proveedores ofrezcan las características de calidad anunciadas, y para aquellos que necesitan encontrar las compensaciones adecuadas entre los niveles de QoS y los costos operacionales.

1.5.2 Revisión sobre el software de monitoreo existente

En el mercado actual existen gran variedad de herramientas para el monitoreo con diferentes capacidades y utilidades. A continuación, se presentan unas de ellas.

1.5.2.1 ZABBIX

La herramienta Zabbix es usada para monitoreo distribuido, es de código abierto de clase empresarial. Este software monitorea un gran número de parámetros de red, el estado e integridad de servidores, servicios TI, máquinas virtuales, aplicaciones, bases de datos, sitios web, la nube, entre otros. Zabbix utiliza notificaciones flexibles que ayudan a los usuarios a configurar alertas basadas en correo electrónico; esta herramienta ofrece funciones de visualización de datos recopilados [40].

Zabbix posee una interfaz web para que el usuario interactúe con ella, donde puede ver el estado de la red de datos y sus equipos servidores. Esta herramienta está compuesta por un servidor, almacenamiento de base de datos, proxy y agente. El servidor se encarga de que los agentes informen sobre la disponibilidad y la integridad de la red, el almacenamiento de la base de datos guarda la información recopilada y el agente captura e informa los datos recopilados al servidor. Zabbix es una herramienta gratuita, y distribuida bajo la licencia pública general GPL versión 2.

1.5.2.2 NAGIOS CORE

Nagios core es una herramienta que permite monitorear elementos de infraestructura TI, protocolos de red, definir métricas para hardware, es intuitiva y de fácil configuración, sus elementos ayudan a hacer la revisión de HTTP, Protocolo de Oficina de Correo (POP3, *Post Office Protocol*), Protocolo de Acceso a Mensajes de Internet (IMAP, *Internet Message Access Protocol*), Protocolo de Transferencia de Archivos (FTP, *File Transfer Protocol*) y Capa Segura (SSH, *Security Shell)* [41]. Esta herramienta utiliza plugins para la revisión del estado de los componentes que se están monitoreando, ellos envían la información recolectada hacia NAGIOS, además son los encargados de realizar las comprobaciones del estado de los servicios TI. Está diseñado para regresar y enviar los datos capturados a aplicaciones externas para procesar y visualizarlos. Nagios core, es una herramienta para monitoreo de red, de código abierto. Está licenciado bajo la GPL General Public License Version 2.

1.5.2.3 SOLARWINDS

La herramienta Solarwinds es un software de gestión de TI que ofrece licenciamiento perpetuo o por suscripción; en el primer caso, se puede usar el software de manera indefinida y el segundo, se basa en plazos de tiempo definidos y el uso de la herramienta se realiza durante el periodo que se canceló. Solarwinds se centra en servicios e

infraestructura TI, ofrece características como la correlación de eventos de los sistemas, aplicaciones, y red [42], además brinda opciones para la captura, análisis de Logs que son usados para encontrar fallos en corto tiempo. Solarwinds posee opciones para el monitoreo del desempeño de servicios e infraestructura TI, mediante la captura de información en tiempo real de los elementos que soportan los servicios TI tales como: router, switches, firewalls, servidores, computadores, etc.; por otro lado, Solarwinds brinda la capacidad de generar alertas que se pueden enviar vía correo electrónico, los tipos de alerta que maneja son: consumo de recursos hardware como CPU, memoria RAM, capacidad de almacenamiento en el disco duro, fallos, interrupciones e indisponibilidad de los servicios TI.

1.5.2.4 PRTG

PRTG es una herramienta para el monitoreo integral que permite supervisar una gran cantidad de dispositivos que tengan una dirección IP, dentro de los parámetros de supervisión se encuentran métricas como el uso de CPU, uso de memoria RAM, ancho de banda, cantidad usada y disponible del disco duro [43].
Esta solución para monitoreo está compuesta por un servidor web y sondas, en el servidor se configuran, administran los datos y las sondas de captura de la información y monitorean las variables de los dispositivos donde se instalaron.

PRTG necesita credenciales para acceder a los dispositivos de la red a monitorear. Durante el proceso de instalación local de PRTG, se agregan automáticamente dispositivos con algunos sensores predeterminados para hacer funciones de monitoreo.

1.5.2.5 ELASTIC STACK

Elastic Stack es una herramienta para búsqueda, monitoreo de redes, computadores, equipos de red, etc., que ofrece a los usuarios observar, monitorear todos los elementos de la infraestructura de las empresas por medio de la unificación de métricas y logs, los cuales son almacenados en tiempo real en el stack, para posteriormente buscarlos y analizarlos mediante la función de *Machine Learning* que está integrada a la herramienta. La funcionalidad de *Machine Learning* permite encontrar valores atípicos, tendencia y anomalías en los datos que se han capturado.
Elastic Stack es una herramienta que tiene dos líneas de operación la primera es la opción open source (*open source*, código abierto) la cual se puede descargar directamente de la página oficial, a ella se le puede hacer modificación del código y mejorar sus capacidades.

Si bien la herramienta es open source, no implica que todas las funcionalidades de la misma sean de libre acceso. Dentro de la herramienta, en la versión 7.8.1, existen funciones específicas que se deben adquirir previo pago para poder hacer uso de estas, por ejemplo, módulo *Machine Learning*.

La segunda opción de operación de la herramienta se conoce con el nombre ECLOUD; esta es una solución que se crea y almacena en la Nube pública a través de dos proveedores grandes AWS (Amazon Web Services) y Google Cloud. Al elegir esta opción se debe pagar por los recursos hardware del servidor principal.

Elastic stack es un conjunto de productos compuestos por *beats, Elasticsearch, Kibana, Logstash* como se muestra la Figura 1, a la combinación de estos tres últimos se le conoce en el mercado como ELK la cual tiene la siguiente estructura.

Figura 1. Elementos principales de la herramienta ELASTIC STACK

1.5.2.5.1 ELASTICSEARCH

Elasticsearch es un motor de búsqueda y análisis de datos, permite buscar, almacenar, y analizar una gran cantidad de datos de manera rápida y casi en tiempo real. *Elasticsearch* es un repositorio donde se almacena toda la información capturada o recopilada por los *beats* o *Logstash* [44]. El motor de búsqueda que tiene *Elasticsearch* está basado en Lucene, este último es una API (*Application Programming Interface*) que permite la recuperación de información. Un aspecto importante de Lucene es que brinda una independencia en el formato del fichero al trabajar con documento que tiene campos. Los ficheros de datos que se usan son en formato JSON (*JavaScript Object Notation*).

1.5.2.5.2 KIBANA

Kibana es una plataforma de análisis y visualización de código abierto diseñada para trabajar con *Elasticsearch.* El módulo *Kibana* se usa para buscar, ver e interactuar con los datos almacenados en los índices de *Elasticsearch*.
Kibana es la interfaz gráfica en donde se visualiza la información recolectada y procesada, posee las siguientes herramientas: Discover, Visualice, Dashboard, Canvas, Machine Learning, Logs APM, entre otros [45].

- **Discover:** en esta sección se pueden ver los datos que se están recolectando en Elasticsearch.
- **Visualice:** en esta sección se crean las visualizaciones a partir de los datos capturados.
- **Dashboard:** en esta sección se crean y diseñan los tableros con las visualizaciones creadas anteriormente, como se muestra en la Figura 2.
- **Machine Learning:** esta sección permite hacer estudios de *machine learning* con los datos que han sido capturados y almacenados en *Elasticsearch*, para realizar análisis de comportamientos anómalos.
- **Logs:** en esta sección se encuentra en una interfaz gráfica con la información de los Logs capturados.

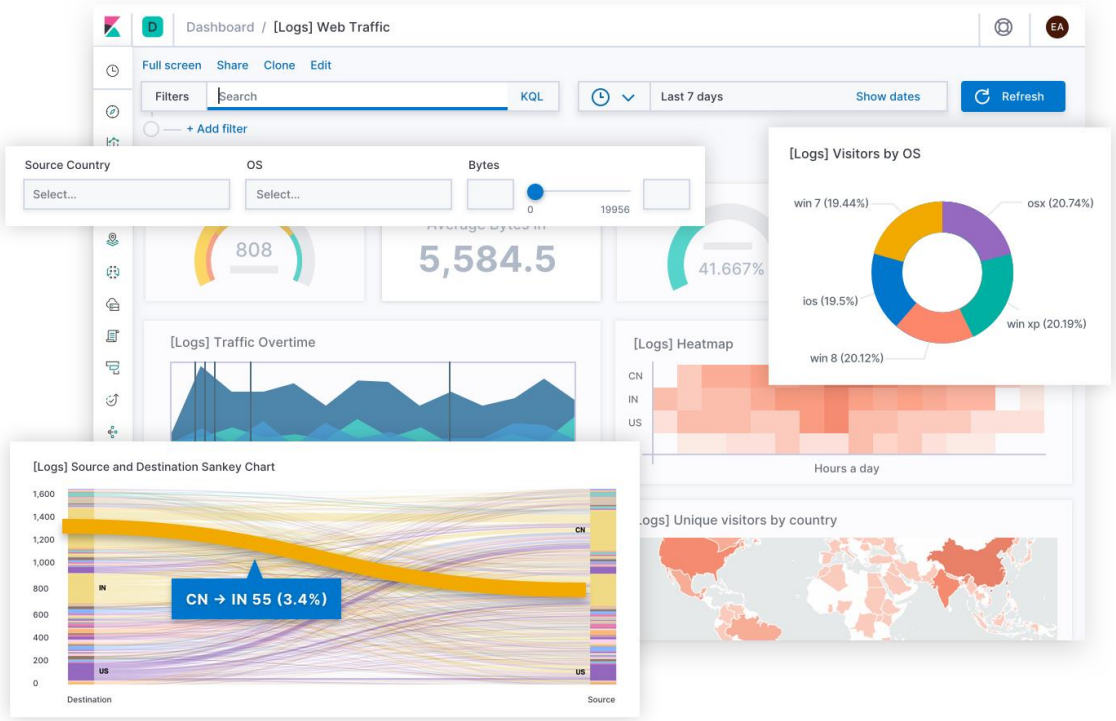

Figura 2. Ejemplo de dashboard en la herramienta ELASTIC STACK

1.5.2.5.3 LOGSTASH

Logstash es un motor de recopilación de datos de código abierto con capacidades de canalización (recoger toda la información de varias fuentes y enviarlas por un solo camino hacia *Elasticsearch*) en tiempo real, este módulo permite unificar dinámicamente los datos de diferentes fuentes, normalizando los datos en los destinos de su elección. *Logstash* permite capturar información de manera no intrusiva por medio de sus diferentes tipos de entradas que soporta, por ejemplos: snmp, syslog, beats, file, github, http, imap, irc, java_generator, java_stdin, jms, jmx, Kafka, redis, snmptrap, stdin, tcp, udp, xmpp, entre otros.

Logstash no solo es un complemento para ingesta de información, este tiene otras características importantes como el enriquecimiento y transformación de información para dar más claridad sobre los datos a obtener, esto se hace a través de filtros como mutate, ruby, rename, geoip, entre otros [46]. La Figura 3 esquematiza las facilidades que tiene *Logstash.*

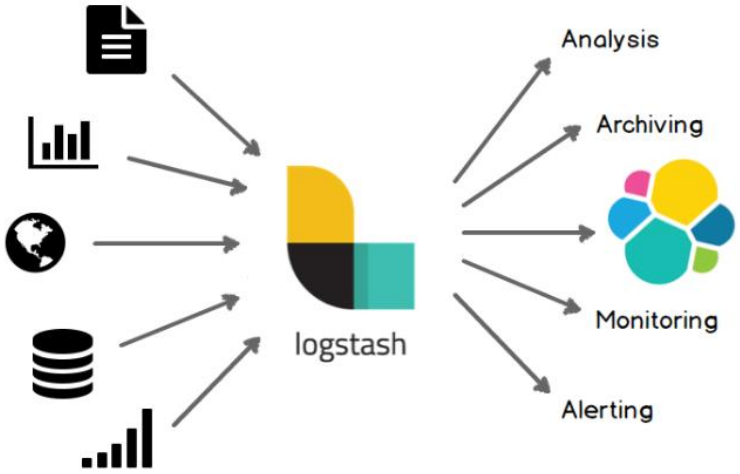

Figura 3. *Logstash* motor de replicación de información

1.5.2.5.4 BEATS

Beats son agentes que se instalan para recolectar información de los equipos que se desean analizar, estos agentes recopilan información de métricas de hardware, red entre otros. Los agentes se pueden instalar sobre Windows, linux, y MacOs. A continuación, se listan los principales beats: *metricbeat, packbeat, winlogbeat, filebeat, heartbeat, auditbeat* [47].

Metricbeat: este agente permite recolectar información de sistema por ejemplo CPU, memoria RAM, disco duro, mediciones del sistema operativo y servicio utilizados [48].

Packetbeat: permite analizar los paquetes de red en tiempo real, esta información se utiliza en *Elasticsearch* hacer un análisis de rendimiento, monitoreo. Este agente captura el tráfico de red entre sus servidores de aplicaciones y servicios, además puede correlacionar las solicitudes con las respuestas, y es un complemento importante para dar visibilidad entre los servidores de su red [49].

La tarea principal de *packetbeat* es detectar el tráfico entre los equipos servidores y que estén dentro de la red, para analizar los protocolos de nivel de aplicación sobre la marcha correlacionando los mensajes en transacciones. Packetbeat; admite los siguientes protocolos para capturar información: ICMP (v4 y v6), Protocolo de Configuración Dinámica (v4) (DHCP*, Dynamic Host Configuration Protocol)*, Sistema de Nombres de Dominio (DNS, *Domain Name System*), HTTP, Cassandra, Mysql, PostgreSQL, Redis, Thrift-RPC, MongoDB, Memcache.

Winlogbeat: es un agente que captura los registros de eventos de Windows, este agente puede leer de uno o más registros de eventos haciendo uso de las API de Windows, tiene funciones para filtrar los eventos según los criterios configurados por el usuario para ver solo la información más relevante [50]. Eventos tales como: de aplicación, de hardware, de seguridad, del sistema.

Auditbeat: es un agente ligero muy importante dentro del conjunto de Beats, ya que permite auditar las actividades de los usuarios, los procesos en los equipos servidores y clientes, el agente recopila, centraliza eventos de auditoría desde Linux Audit Framework, su uso más frecuente es para detectar cambios en archivos importantes de configuración de los sistemas basados en Linux, que contienen información sensible y crítica de la empresa, por ejemplo archivos binarios, además puede identificar posibles violaciones de la política de seguridad [51].

Heartbeat: es un agente liviano que se instala y configura en un servidor remoto para poder monitorear periódicamente el estado de los servicios examinando si estos están disponibles o son accesibles, este agente es de gran interés cuando se requiere verificar que se esté cumpliendo con los acuerdos de nivel de servicio(SLA) para el tiempo de actividad del servicio. Por otro lado, este agente es muy útil para casos de uso de seguridad, por ejemplo, cuando se necesita verificar que ninguna persona del exterior a nuestra organización o empresa pueda acceder a los servicios en su servidor empresarial privado [52].

Heartbeat admite monitores para verificar equipos terminales por medio de:

- Solicitudes de eco ICMP (v4 y v6). Se usa el monitor icmpmonitor cuando simplemente desee verificar si un servicio está o no disponible.
- TCP, se usa el monitor tcpmonitor para conectarse por medio de TCP, se puede configurar este monitor para verificar el punto final enviando y / o recibiendo una carga útil personalizada.
- HTTP, se usa el monitor httpmonitor para conectarse mediante HTTP, se puede configurar para verificar que el servicio devuelva la respuesta esperada, como un código de estado específico, encabezado de respuesta o contenido.

Filebeat: este agente permite recolectar toda información acerca de registros de eventos en el sistema operativo o de cualquier dispositivo que los genere; tiene un uso especial para capturar los log dentro los equipos que hacen uso de sistemas Linux como se ve en la Figura 4, con esta información se puede tener una visión más específica cuando se presentan errores de los cuales se desconoce la razón [53].

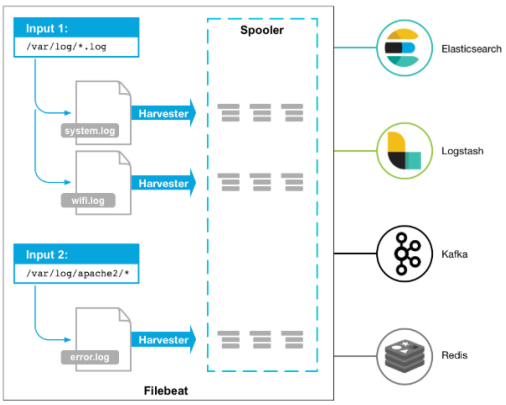

Figura 4. Captura de Logs con *filebeat*

A continuación, se presenta la Tabla 3 donde se encuentran las características generales de algunas herramientas software para el monitoreo de redes y servicios TI.

CARACTERÍSTICAS	HERRAMIENTAS				
	Zabbix	Nagios core	SOLARWINDS	PRTG	Elastic stack
Sistemas operativos usados	Windows Linux	Windows Linux	Windows Linux	Windows Linux	Windows Linux iOS
Tipo de Licencia	Código abierto	Código abierto	Paga	Código abierto	Código abierto
Elementos que permite monitorear	Parámetros de red, la salud e integridad de servidores, servicios TI, máquinas virtuales, aplicaciones, bases de datos, sitios web	Computadores, router, switch, aplicaciones móvil y web	Computadores, router, switch, aplicaciones móvil y web	Computadores, router, switch, aplicaciones móvil y web	Computadores, router, switch, aplicaciones móvil y web
Lenguaje de programación de la herramienta	C, PHP, java	Perl, C	No especifica	C++, Visual studio	Apache lucence
Facilidad de Visualización de Resultados	si	si	si	si	si
Manejo de Alertas	Correo electrónico	Correo electrónico Pager dutty SMS Audio	Correo electrónico, internas de la herramienta	Correo electrónico, internas de la herramienta	Correo electrónico, alertas a aplicaciones como Slack, Pager dutty, internas dentro de la herramienta

Tabla 3. Comparación de características de herramientas para monitoreo de red y servicios TI

Las razones por la cuales se seleccionó la herramienta Elastic Stack son las siguientes:

- La empresa KEYNETTIC S.A.S. había seleccionado previamente la herramienta Elastic Stack para propósitos de monitoreo de red, con fines de fortalecer su proceso de consultoría.
- La herramienta Elastic Stack es robusta, flexible, modular y permite su instalación en varios sistemas operativos.
- Elastic Stack cuenta con alertas y notificaciones para informar en tiempo real de problemas y fallas de los dispositivos que se están monitoreando.
- Elastic Stack brinda flexibilidad en la configuración de los recursos necesarios para su ejecución en la nube.

2. CAPÍTULO II. Metodología

Para el desarrollo del proyecto se hace uso del manual de buenas prácticas para la gestión de proyectos PMI [54] [55], por medio de ellas se desarrolla el proyecto de forma gradual permitiendo la ejecución organizada del mismo a través de cinco procesos: iniciación, planificación, ejecución, supervisión, control y cierre.

2.1 Proceso de iniciación

En esta fase se da comienzo el proyecto, se determina la idea, los requerimientos y se estima como se va a llevar a cabo. Este proceso es importante para lograr el éxito en el proyecto, ya que el mal planteamiento de los objetivos podría influir en el fracaso del mismo.

Inicialmente se realizaron dos reuniones presenciales en la cuidad de Bogotá Colombia, con la empresa cliente de Keynettic S.A.S, en ellas se presentó el proyecto, también se establecieron los requerimientos por parte de la empresa. La idea principal del proyecto es adaptar una herramienta para medir el desempeño de los servicios TI, los requerimientos se presentan en la sección 2.1.1.

2.1.1 Requerimientos de la empresa

En esta etapa del proyecto se establecen los requerimientos funcionales y no funcionales que debe tener la herramienta adaptada para medición de servicios TI, estos son definidos por KEYNETTIC S.A.S y por su cliente. Los requerimientos funcionales se definen como los servicios, funciones que debe ofrecer la herramienta adaptada, mientras que los requerimientos no funcionales se definen como aquellos que no son necesariamente funciones particulares de la herramienta adaptada, sino características como disponibilidad, fiabilidad, seguridad, etc. [56]. En la sección 2.1.1.1, 2.1.1.2 se presentan los requerimientos funcionales y no funcionales que se establecieron inicialmente.

2.1.1.1 Requerimientos funcionales

- Visibilizar las métricas de consumo de recursos de los equipos de la empresa cliente KEYNETTIC S.A.S a través de paneles.
- Monitorear métricas de consumo, así como los KPI de servicios y equipos en tiempo real.
- Capturar los logs del switch Cisco SG500-52 52-port Gigabit Stackable.
- Aplicar *Machine Learning* para la detección de comportamientos anómalos con base en los datos recolectados.

2.1.1.2 Requerimientos no funcionales

- Cifrar el envío de la información.
- Ofrecer alta disponibilidad de la herramienta para de medición del desempeño de servicios TI de la empresa cliente de KEYNETTIC S.A.S

2.2 Proceso de planificación

En esta etapa se planifican las actividades necesarias para la realización del proyecto, las tareas y sus funcionalidades. Teniendo en cuenta lo anterior se definen las siguientes actividades para cumplir los requerimientos planteados en la sección 2.1.

- Solicitar el esquema de la infraestructura de TI a la empresa cliente de KEYNETTIC S.A.S.
- Formulación de KPI.
- Criterios de selección de la herramienta *Elastic Stack* para implementarla en un servidor público o privado.
- Planteamiento de la infraestructura de trabajo para dar cumplimiento a los requerimientos funcionales.
- Definición de requerimientos mínimos hardware para implementar y adaptar la herramienta.

2.2.1 Infraestructura TI de la empresa

En esta sección se presenta la infraestructura TI de la empresa cliente de KEYNETTIC S.A.S. La empresa utiliza servicios tales como Voz sobre IP (VoIP), Circuito Cerrado de Televisión (CCTV) y SIIGO, sobre la que se midió el desempeño de servicios TI que ofrece. En la Figura 5, se muestra la infraestructura de referencia.

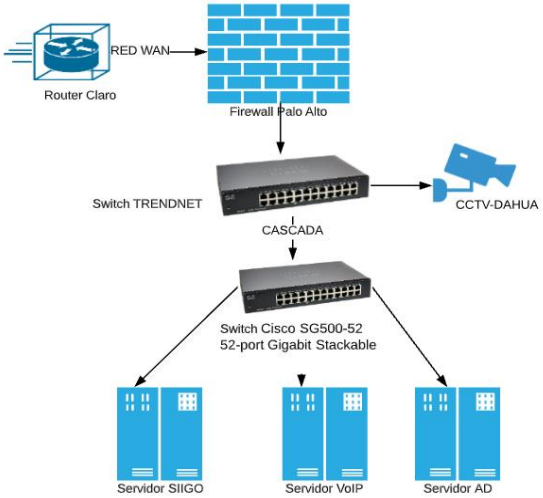

Figura 5. Infraestructura de la empresa cliente de KEYNETTIC S.A.S.

La infraestructura descrita está conformada por los dispositivos de red que se describen en la Tabla 4.

Equipos y dispositivos de red	Cantidad
Servidor SIIGO	1
Servidor VoIP	1
CCTV DAHUA	1
Switch TRENDNET	1
Firewall Palo Alto	1
Servidor AD	1
Router Claro	1
Switch CISCO SG500-52 52-PORT GIGABIT STACKABLE	1

Tabla 4. Dispositivos de red de la empresa cliente de KEYNETTIC S.A.S

2.2.2 Formulación de KPI

En esta sección se presenta la definición de los KPI, los cuales se usaron para medir el desempeño de los servicios TI de la empresa cliente KEYNETTIC S.A.S; dicha definición se hizo por medio del uso de las recomendaciones de ITIL versión 4 [25], la sección *Measuarebles and reporting***,** que plantea cuatro pasos para lograrlo, los cuales se describen a continuación:

1. Fijar un objetivo.
2. Identificar factores de éxito.
3. Selección de métricas y herramientas de medición.
4. Formar sistema de indicadores.

Para cada objetivo se define un conjunto de indicadores clave del desempeño (KPI), que se notaran por la letra ***K*** y un número correspondiente, adicional a esto, se establecen valores objetivo de referencia (***Target***) denotados con la letra ***T*** y su número correspondiente con un umbral máximo a tolerar(***Threshold***) denotados con la letra ***M*** y su correspondiente número.

2.2.2.1 Definición de KPI para el equipo servidor de VoIP

2.2.2.1.1 Fijar objetivo número 1

Visibilizar la información del uso de la capacidad de recursos hardware del servidor que soporta VoIP.

2.2.2.1.2 Identificación factores de éxito para el objetivo número 1

- Identificar procesos que generen alto consumo de recursos CPU y memoria RAM que se estén ejecutando en el equipo servidor de VoIP.
- Generar alertas tempranas cuando el uso de la capacidad de recursos hardware de CPU y memoria RAM del servidor que soporta el servicio VoIP, sea mayor o igual al 80% de los recursos totales instalados.

2.2.2.1.3 Selección de métricas y herramientas de medida para el objetivo número 1

En la sección 2.2.2.1.2 se identificaron los factores claves éxito para cumplir el objetivo número 1, con ellos se definen los KPI para el servidor VoIP, representados con las letras ***K1*** y ***K2*** y sus valores objetivos (***Target***) ***T1*** y ***T2*** y sus umbrales Threshold ***M1*** y ***M2***. Estos valores se observan en la Tabla 5.

- Porcentaje de consumo de CPU por procesos ejecutado en el servidor VoIP, ***K1***.
- Porcentaje de consumo de memoria RAM por proceso ejecutado en el servidor VoIP, ***K2***.

KPI	Target	Threshold
K1	**T1=50%**	**M1=80%**
K2	**T2=50%**	**M2=80%**

Tabla 5. KPI para el servidor de VoIP

2.2.2.2 Definición de KPI para el consumo de recursos de red

2.2.2.2.1 Fijar objetivo número 2

Informar del consumo (capacidad) en tiempo real del switch Cisco SG500-52 52-port Gigabit Stackable.

2.2.2.2.2 Identificar factores de éxito para el objetivo número 2

- Capturar métricas de red del switch Cisco SG500-52 52-port Gigabit Stackable para conocer su consumo.
- Observar métricas de red del switch Cisco SG500-52 52-port Gigabit Stackable.
- Detectar consumos superiores al 80% en la capacidad de recursos de red.
- Detectar cuando la capacidad de recursos de red que soporta el servicio de VoIP este en rango de consumo superior el 80%.

2.2.2.2.3 Selección de métricas y herramientas de medida para el objetivo número 2

En la sección 2.2.2.2.2 se identificaron los factores claves éxito para cumplir el objetivo número 2, con ellos se crean los KPI para el switch Cisco SG500-52 52-port Gigabit Stackable, representados con las letras ***K3***, ***K4***, ***K5***, ***K6***, ***K7***, ***K8***, sus valores objetivos (***Target***) ***T3***, ***T4***, ***T5***, ***T6***, ***T7***, ***T8*** y sus umbrales (***Threshold***) ***M3***, ***M4***, ***M5***, ***M6***, ***M7***, ***M8***, estos valores se pueden observar en la Tabla 6.

- Cantidad de tráfico de red entrante en el switch Cisco SG500-52 52-port Gigabit Stackable, ***K3***.
- Cantidad de tráfico de red saliente en el switch Cisco SG500-52 52-port Gigabit Stackable, ***K4***.
- Cantidad de paquetes entrantes en cada puerto del switch, ***K5***.
- Cantidad de paquetes salientes en cada puerto del switch, ***K6***.
- Cantidad de paquetes descartados entrantes en cada puerto del switch, ***K7***.
- Cantidad de paquetes descartados salientes en cada puerto del switch, ***K8***.

KPI	Target	Threshold
K3	**T3=50%**	**M3=80%**
K4	**T4=50%**	**M4=80%**
K5	**T5=50%**	**M5=80%**
K6	**T6=50%**	**M6=80%**
K7	**T7=50%**	**M7=80%**
K8	**T8=50%**	**M8=80%**

Tabla 6. KPI del consumo de recursos de red

2.2.3 Criterios de selección para implementar *Elastic Stack* en un servidor público o privado

La herramienta *Elastic Stack* permite que se puedan implementar los desarrollos y proyectos en servidores privados o servidores públicos.
Los servidores privados son equipos dentro de la organización, en una red de área local LAN, en el cual se instala y configura *Elastic Stack* (*Elasticsearch y Kibana*) para almacenar

los datos capturados con los agentes *Beats*; estos equipos hacen uso de los recursos hardware de la empresa; otro aspecto a tener en cuenta es que cuando se usa de forma local, el servidor privado *Elastic Stack* permite al usuario descargar *Elasticsearch y KIbana* de forma gratuita con funciones limitadas, pero permite adquirir un licenciamiento para hacer uso completo de las funcionalidades de ella.

Los servidores públicos o la opción *ECLOUD* (*Elastic CLOUD*) es un equipo que se implementa en una nube pública tipo AWS, Google Cloud o Microsoft Azure, el cual hace uso de los recursos hardware de alguno, estos tres grandes proveedores. Por su uso se debe pagar una tarifa que depende de tres factores que son: primero, el proveedor que se elija; segundo, las características hardware que se van a usar (*Elastic Stack* tiene en la web un portal para calcular el precio de los recursos que se van a usar antes de hacer la implantación [4]), y tercero, el tipo licenciamiento (ver en la Tabla 11).

La versión *Elastic CLOUD* ofrece acceso completo a las funcionalidades de la herramienta *Elastic Stack*, entre ellas encontramos: seguridad, backup, geolocalización, capturar y enviar los datos a cualquier parte del mundo donde este implementado el servidor. A continuación, la Tabla 4 muestra la comparación de algunas características al implementar en las dos modalidades.

Tipo	Servidor público	Servidor privado
Aumentar capacidad hardware (memoria RAM, almacenamiento)	Dinámica bajo demanda.	Manual para servidor físico. Dinámica para servidor sobre máquinas virtuales.
Funcionalidades	Completa con el licenciamiento(visualizaciones, alertas, captura de información, *Machine Learning*).	Capacidades básicas de la herramienta (visualización, captura de información).
Cifrado de información	Cifrado de la información servidor cliente	Cifrado de la información servidor cliente.
Envió de información	Cualquier parte donde haya conexión a internet	Interna en la empresa u organización .
Costo	Se debe pagar por el uso de los recursos hardware de los proveedores en la nube AWS, Google Cloud o Microsoft Azure	Sin costo porque usa recursos hardware dentro de la organización.

Tabla 7. Comparación de implementación de la herramienta *Elastic Stack* en un servidor público y privado.

La empresa KEYNETTIC S.A.S y estudiante, decidieron trabajar con el servidor público de *Elastic Stack,* en su versión *Elastic Cloud,* tomando como referencia la Tabla 7, ya que con esta versión se tiene acceso a la funcionalidad completa de la herramienta y se puede trabajar de forma remota.

2.2.4 Planteamiento de la infraestructura de trabajo y requerimientos mínimos hardware para implementación del servidor *Logstash*

En esta sección se muestra y describe la infraestructura desplegada para el desarrollo del proyecto, teniendo en cuenta los requerimientos del mismo, la ubicación regional de la empresa donde se ejecuta la práctica profesional junto con uso de *Elastic Cloud*. La Figura 6 describe el diagrama esquemático de la infraestructura utilizada, y las tablas 8 y 9 indican los componentes de red utilizados, su ubicación, las características hardware del servidor *Logstash* respectivamente.

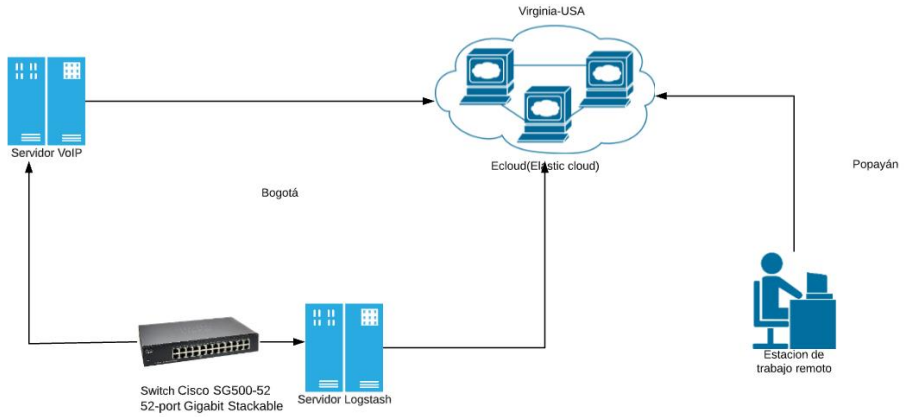

Figura 6. Infraestructura para el desarrollo del proyecto

Equipos y dispositivos de red	Cantidad	Ubicación
Servidor VoIP	1	Bogotá (Colombia)
Switch Cisco SG500-52 52-Port Gigabit Stackable	1	Bogotá (Colombia)
Servidor *Logstash*	1	Bogotá (Colombia)
ECLOUD (*Elastic Cloud*)	1	Virginia (USA)
Estación de trabajo remoto	1	Popayán (Colombia)

Tabla 8. Lista de elementos de la Infraestructura para el desarrollo del proyecto

Nombre	Características
Procesador	2 núcleos
Disco duro	500GB
Memoria RAM	8 Gigabytes

Tabla 9. Características hardware de los equipos para usar *Logstash* y estación remota.

2.3 Proceso de ejecución

Dentro del proceso de ejecución se pone en marcha el desarrollo del Proyecto, se pretende llevar a práctica la planificación realizada previamente. Es importante que durante la ejecución del proyecto exista una comunicación eficiente entre quien adapta la herramienta, el equipo de trabajo de la empresa KEYNETTIC S.A.S y el equipo de ingeniería de la empresa monitoreada, para tomar decisiones lo más rápido posible frente a cualquier problema que surja. Además, se deben organizar, programar periódicamente reuniones

para administrar las tareas y actividades del proyecto, para socializar regularmente el progreso del mismo e identificar las prioridades siguientes.

En esta sección se presenta la información sobre el proceso de ejecución del proyecto, las actividades que se llevaron a cabo para dar cumplimiento a la medición del desempeño de servicios TI, los cuales van a ser monitoreados mediante los KPI definidos anteriormente.

En la sección 2.2.1 se presentó la infraestructura de la empresa junto con los servicios de los cuales hace uso, pero de estos servicios y dispositivos de red se decidió trabajar sobre el servicio de VoIP el cual involucra el switch Cisco SG500-52 52-port Gigabit Stackable.

La decisión de trabajar con un solo servicio, de todos los que suministraba la empresa, acorde al ingeniero a cargo de esta área, se dio en razón a que el servidor de VoIP era el único de todos ellos que contaba con respaldo tanto del software para la restauración del sistema como de los datos que se encontraban dentro del mismo servidor (estas copias de respaldo y backup de configuraciones, se recomienda que sean almacenadas en disco duro extraíble o en otro computador). Contar con este respaldo disminuiría los posibles problemas de operación en caso de que se presentaran fallas en el proceso de adaptación y validación de la herramienta, por ejemplo, debido a que la medición sobre el servicio de VoIP se realiza en producción y en tiempo real los cambios se hacen directamente en el servidor de VoIP y en caso de que las configuraciones generen un problema y afecten el servicio, se podrá dar continuidad sin grandes problemas y en corto tiempo.

Anteriormente se definió con que servicios y dispositivos de red se trabaja, el paso siguiente consiste en la adaptación de la herramienta *Elastic Stack*, esta información será presentada en la sección 3 llamada “Adaptación de la herramienta *Elastic Stack*”.

2.4 Proceso de supervisión y control

El fin de este proceso es garantizar que los objetivos sean alcanzados, por medio de una buena supervisión para que se puedan tomar decisiones y acciones correctivas si se están presentando inconvenientes. El proceso de supervisión y control es llevado por el ingeniero encargado de la empresa KEYNETTIC S.A.S., para llevarlo a cabo se realizaron reuniones virtuales por medio de la herramienta ZOOM, para presentar los reportes y avances de los requerimientos solicitados en la sección 2.1.

2.5 Proceso de cierre

Este es el último proceso y culminación del proyecto. Todos los proyectos poseen una existencia temporal, y termina cuando se cumple con lo establecido. Se hacen pruebas finales de corrección de la solución. En esta etapa se hace entrega de la herramienta *Elastic Stack* adaptada para medir el desempeño de servicios TI de la empresa cliente KEYNETTIC S.A.S.

3. CAPÍTULO III. Adaptación de la herramienta *Elastic Stack*

Para adaptar de la herramienta *Elastic Stack*, con el fin de medir desempeño del servicio de VoIP, se diseñó un diagrama de bloques con las funcionalidades que debe tener el sistema para que cumpla con los objetivos detallados en la sección 2.1. Cada bloque descrito constituye la adaptación de las funcionalidades de la herramienta *Elastic Stack*, las cuales permiten recopilar datos en bruto de las fuentes para procesarlos y ofrecer información de valor agregado para analizar el estado de los servicios que usa la empresa. El diagrama en bloques de las funcionalidades consideradas para el proceso de adaptación de la herramienta *Elastic Stack* se describe en la Figura 7.

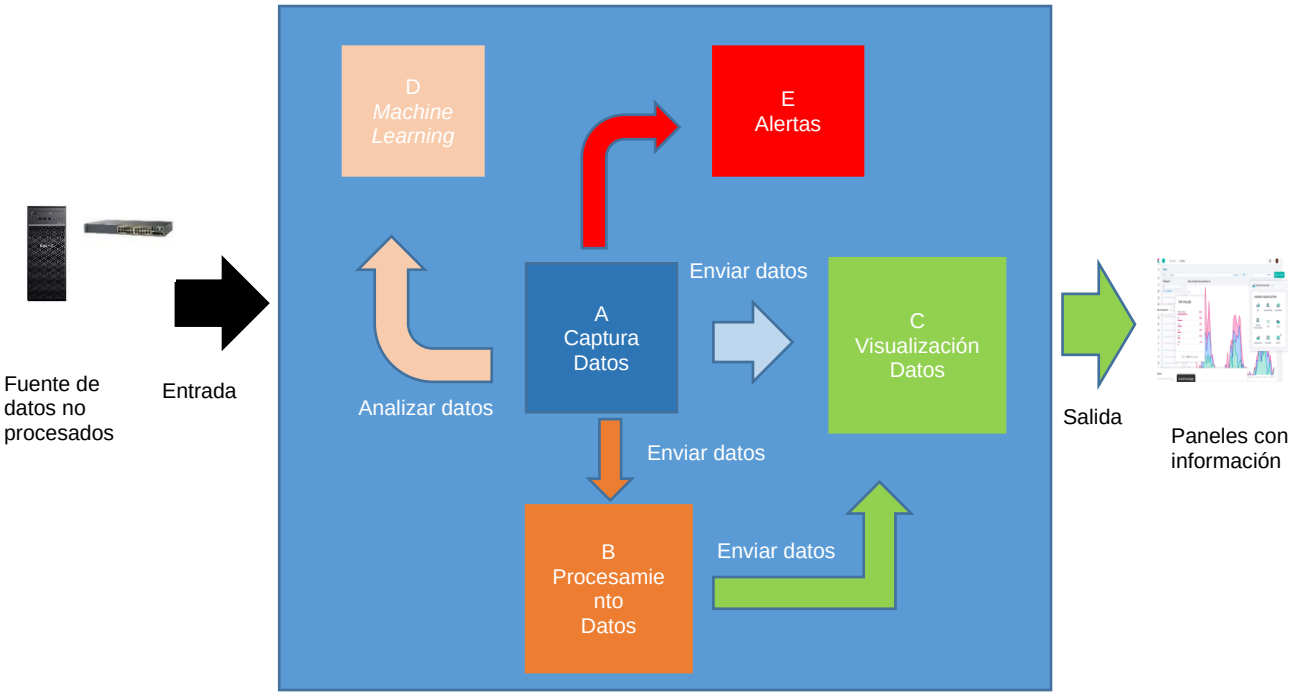

Figura 7. Diagrama bloques del sistema para la medición del desempeño de servicio TI

3.1 Captura Datos

El bloque A, realiza la captura y recopilación de los datos en bruto que entregan las fuentes de interés. La Tabla 10 describe las fuentes de datos y el elemento de *Elastic Stack* que se encarga de recibirlos, estos datos se envían al bloque B para hacer una transformación de ser necesario, este proceso se muestra en la Figura 8.

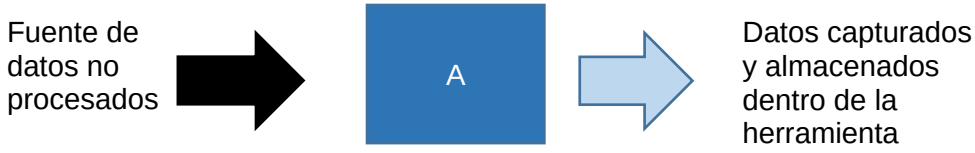

Figura 8. Bloque A captura de datos

Fuente de datos	Elementos de *Elastic Stack*
Servidor VoIP	*Metricbeat, filebeat*
Switch Cisco SG500-52 52-port Gigabit Stackable	*Logstash*

Tabla 10. Fuente de datos de entrada al bloque A

Funcionamiento

En el bloque A ingresa toda la información sin procesar procedente de las fuentes descritas en la Tabla 10. Dentro del bloque se presentan dos casos de tipo de información, la primera es el denominado caso 1 que es la entrada de datos del servidor de VoIP para la cual se usan los elementos *metricbeat* y *filebeat* de la herramienta *Elastic Stack*, y para el caso 2 que corresponde a los datos del switch Cisco SG500-52 52-port Gigabit Stackable se emplea Logstash.

- **Caso 1:**

En este caso la entrada de datos proviene del servidor de VoIP, para este tipo de entrada se usan los elementos *metricbeat* y *filebeat*, el primero se emplea para capturar todos los datos de métricas de CPU, memoria RAM, disco duro, recursos hardware, etc., y el segundo se usa para la captura de Logs dentro del servidor VoIP, y la salida del bloque A será almacenada en *Elasticsearch*, donde posteriormente se crearán las visualizaciones de estos datos.

- **Caso 2:**

La segunda fuente datos es el switch Cisco SG500-52 52-port Gigabit Stackable, para poder capturar la información se hace uso del elemento *Logstash*, el cual toma los datos que contienen las métricas de red mediante el uso del protocolo SNMP, los datos de Logs se recolectan por medio de syslog. Las anteriores son funcionalidades particulares de *Logstash*. Una vez se recolecta la información se envía al bloque B para hacer el procesamiento de los datos y finalmente ser almacenada en *Elasticsearch.*

3.2 Procesamiento Datos

El bloque B es el encargado de procesar los datos capturados y entregados por el bloque A, estos necesitan ser organizados, adaptados para poder ser usados dentro de las visualizaciones y posterior análisis, como se muestra en la Figura 9.

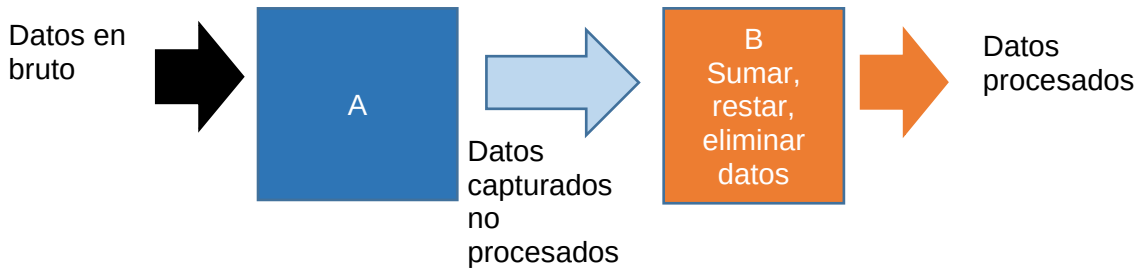

Figura 9. Flujograma envío de datos entre el bloque A y bloque B

Funcionamiento

Los datos que ingresan al bloque B son procesados con funciones y operaciones como: sumar, restar, multiplicar, dividir, cambio de variable, cambio de nombre de variables, eliminar datos, agregar información a los datos, etc., estas funciones son aplicadas a los datos del Switch Cisco SG500-52 52-port Gigabit Stackable específicamente para tres casos particulares que son:

1. Renombrar los campos para las métricas de red capturadas de las OID (*Object Identifier*) de la Tabla 8.
2. Calcular el número de paquetes entrantes y salientes de cada interfaz de red.
3. Adecuar el valor del campo que tiene el estado de la interfaz de red capturado de *ifOperStatus*.

3.3 Visualización Datos

El bloque C es el encargado de crear las visualizaciones con los datos ya procesados del servidor de VoIP y el Switch Cisco SG500-52 52-port Gigabit Stackable, como lo muestra con el flujograma de la Figura 10. Posteriormente las visualizaciones se unirán dentro de paneles Dashboard para tener una vista más completa y gráfica de los datos obtenidos.

Figura 10. Bloque C visualizar datos

Funcionamiento

El bloque C utiliza el elemento *Kibana* que es parte de *Elastic Stack*, dentro de las funcionalidades de *Kibana* se encuentran una gran variedad de plantillas para presentar los datos. El bloque C recibe los datos y por medio *Kibana* los muestra en visualizaciones al usuario final tal como se muestra en la Figura 11. Como se ha mencionado anteriormente se tienen dos tipos de entrada, que son servidor de VoIP y el Switch Cisco SG500-52 52-port Gigabit Stackable para las cuales se realizan las respectivas visualizaciones.

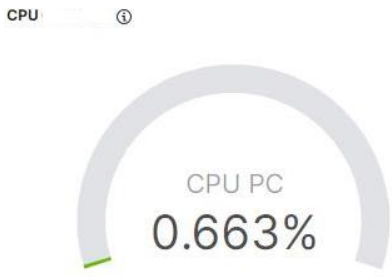

Figura 11. Visualización creada por el bloque C

3.4 *Machine Learning*

El bloque D es el encargado de realizar los estudios de *Machine Learning* con los datos que están almacenados en *Elasticsearch* para correlacionar eventos, detectar valores anómalos y tendencias atípicas que se puedan presentar.

Funcionamiento

El bloque D utiliza los datos en bruto que han sido capturados por el bloquea A, como se aprecia en la Figura 12, por medio de la función ***Machine Learning*** integrada en el elemento *Kibana*. Estos datos son analizados con ciertos parámetros claves, por ejemplo: rango de fecha en el cual se va a realizar el estudio (fecha de inicio y fecha de finalización), nombre del campo que contiene los datos que se van a analizar. Una vez terminado este proceso se ejecuta el estudio y este arroja los resultados del análisis.

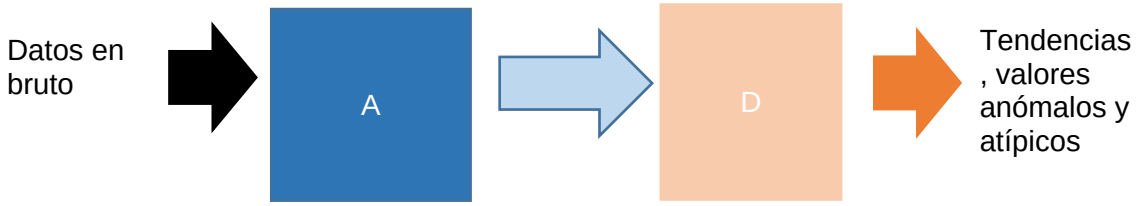

Figura 12. Flujograma de los bloques A y D

3.5 Alertas

El bloque E se encarga de crear las alertas, las cuales envían una advertencia o notificación a la persona encargada del área de servicio, cuando las métricas de los servicios estén sobre pasando el nivel objetivo o cuando en el peor de los casos esté por encima de los valores de tolerancia preestablecidos. Las notificaciones se pueden enviar al correo y aplicación como: Slack y Pager dutty, con las cuales es compatible la herramienta *Elastic Stack* (esta información se ampliará en la sección de implementación de alertas).

4. CAPÍTULO IV. Puesta en funcionamiento de la herramienta *Elastic Stack* adaptada para la medición del desempeño de servicio de VoIP

En esta sección se describe el proceso de puesta en funcionamiento de la herramienta *Elastic Stack* a través de los diferentes módulos que lo van a constituir, mediante las siguientes actividades:

- Dimensionamiento y planeamiento de la capacidad de *Elastic Cloud.*
- Puesta en funcionamiento de *Elastic Stack* y sus funciones para los bloques capturar, transformar, visualizar, Machine Learning y alertas.

4.1. Dimensionamiento de la capacidad de *Elastic Cloud*

La primera actividad para realizar es la puesta en funcionamiento del entorno de operación de *Elastic Cloud*; cuando se realiza este proceso es muy importante hacer la tarea y análisis

del dimensionamiento de la capacidad de los recursos hardware que va usar, ya que anteriormente se mencionó que el costo depende del tipo de proveedor de nube (AWS, Google Cloud, Microsoft Azure), de los recursos hardware seleccionados y del tipo de licenciamiento que se va a usar para el entorno de operación, en la Tabla 11 se presentan el tipo de licenciamiento [58].

Licenciamiento	Características
Estándar	Seguridad en el servidor de *Elastic Stack*, TLS para comunicaciones encriptadas. Funcionalidades de APM, Logs, Metrics, Uptime, Kibana Lens, Maps, Canvas prevención contra malware, todas esta para la solución en Elastic Enterprise Search, Observability y Security. Creación de alertas y acciones en el *Stack*. Prestación de servicio de soporte basado en tickets solo para la versión *Elastic Cloud*.
Oro	Incluye las características de la licencia estándar. Creación de reportes. Acciones de alertas de terceros. Servicio de soporte en horario comercial. Servicio de soporte basado en tickets. SLA de tiempo de respuesta de soporte.
Platino	Incluye las características de la licencia oro. Funcionalidad de *Machine Learning*. Replicación entre clusters. Servicio de Soporte permanente. Servicio de Soporte basado en tickets. SLA de tiempo de respuesta de soporte mejorado.
Enterprise	Incluye las características de la licencia platino. Permite el acceso a *Elastic Endgame*. Ofrece Snapshots buscables. Servicio de Soporte permanente. Servicio de Soporte basado en tickets. SLA de tiempo de respuesta de soporte mejorado.

Tabla 11. Tipo de licenciamiento de *Elastic Cloud*

Teniendo en cuenta la información presentada anteriormente en la Tabla 11 se decide usar para el entorno de operación, el licenciamiento tipo estándar ya que ofrece las funcionalidades necesarias para cumplir con los requerimientos solicitados, el proveedor *Cloud* AWS ubicado en la región N.-Virgina-USA, *Elasticsearch* y *Kibana* en su versión 7.8.1 con los recursos globales presentados en la Tabla 12, terminado el despliegue del

entorno de operación se tiene acceso a las funcionalidades completas de la herramienta *Elastic Stack* por ejemplo Discover, Visualize, Dashboard, *Machine Learning*, Maps.

Elemento	Recursos hardware
Elastic search v.7.8.1	RAM = 1 GB, Almacenamiento = 30GB
Kibana v.7.8.1	RAM = 1 GB
Machine Learning	RAM = 1 GB

Tabla 12. Selección de elementos de la configuración de *Elasctic Cloud*

4.2 Configuración de la adaptación de los bloques

En esta sección se describe la configuración de la adaptación de los bloques presentados en la Figura 7; cada uno con las funciones de *Elastic Stack* y así lograr medir el desempeño de los servicios TI. Los bloques que se configurarán son: bloque captura datos, procesamiento datos, visualización datos, *Machine Learning*, alertas.

4.2.1 Configuración de la adaptación para el bloque captura datos

En la sección 3.1 se presentó el bloque A capturar datos, la configuración de la adaptación de este bloque con las funciones de *Elastic Stack* consta de dos partes ya que se tiene dos fuentes de datos diferentes, una en la cual los datos son del equipo servidor VoIP y la otra el Switch Cisco SG500-52 52-port Gigabit Stackable.

- **Caso 1:**

En primer lugar, se encuentra como fuente de datos el servidor de VoIP, para este equipo se capturan variables hardware, como por ejemplo, CPU usada, memoria de RAM, almacenamiento usado y disponible, etc., y, además se captura los datos de Logs generados por el equipo servidor el cual está sobre el sistema operativo Debian, para las capturas de datos se empelan los elementos *metricbeat* y *filebeat* de *Elastic Stack* respectivamente, estos elementos se instalan y configuran dentro del servidor para capturar los datos; la instalación de *metricbeat* se muestra en el anexo 1.

Una vez realizado lo anterior, se establece la comunicación entre *metricbeat* y el servidor en la nube *Elastic Cloud*, para ello de utiliza las credenciales que genera el entorno de operación cuando es creado, estas se presentan en la Tabla 13 y Figura 13.

Parámetro	Descripción
Cloud.id	ID único del *Elasticsearch* Formato “nombre del desarrollo:ID”
Cloud.auth	Credenciales de usuario Formato (“usuario:passwork”)

Tabla 13. Parámetros para comunicar *Elastic Cloud* con *metricbeat*

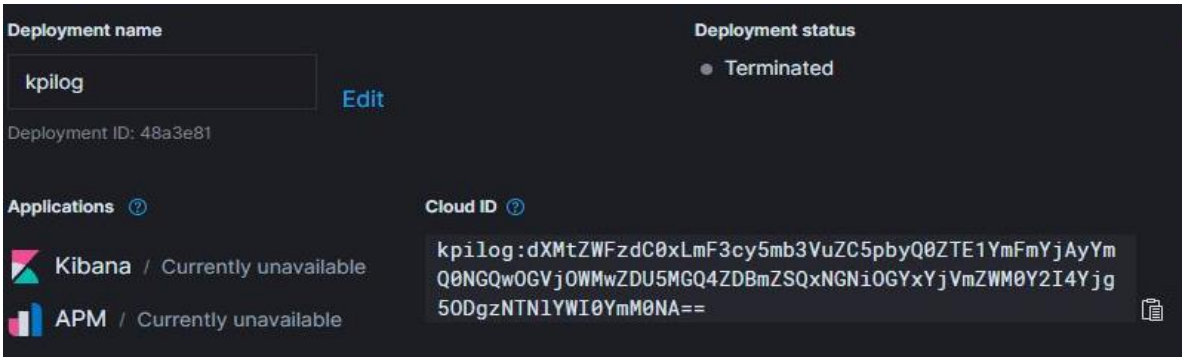

Figura 13. ID del entorno de operación

Una vez terminado el proceso de comunicación, se procede a configurar los parámetros de *metricbeat* para que pueda capturar los datos requeridos. El elemento *metricbeat* tiene varios módulos que permiten capturar diferentes tipos de datos de fuentes, por ejemplo, módulo Oracle, NATS, Ngnix, Tomcat, system, entre otros; para el caso de uso se utiliza el módulo llamado system, este módulo permite capturar los datos del equipo que se mencionó anteriormente; para ello se realiza la configuración que se aprecia en la Figura 14, en la Tabla 14 se describen los parámetros que se configuran para obtener los datos del servidor de VoIP. Después el proceso de captura por parte de *metricbeat*, este envía la información hacia *elasticsearch* donde es almacenada.

```
  GNU nano 2.5.3                                    Archivo: system.yml

# Module: system
# Docs: https://www.elastic.co/guide/en/beats/metricbeat/7.5/metricbeat-module-system.html

- module: system
  period: 10s
  metricsets:
    - cpu
    - core
    - diskio
    - entropy
    - load
    - memory
    - network
    - process
    - process_summary
    - socket
    - socket_summary
    #- entropy
    #- core
    #- diskio
    #- socket
  process.include_top_n:
    by_cpu: 5      # include top 5 processes by CPU
    by_memory: 5   # include top 5 processes by memory

- module: system
  period: 1m
  metricsets:
    - filesystem
    - fsstat
  processors:
  - drop_event.when.regexp:
      system.filesystem.mount_point: '^/(sys|cgroup|proc|dev|etc|host|lib)($|/)'
```

Figura 14. Parámetros de configuración del módulo system de *metricbeat* para capturar los datos de CPU, RAM, disco de almacenamiento

Parámetro	Descripción
Period	Tiempo de muestreo.
cpu	Captura información de la CPU del computador.
core	Captura de información del uso de cada núcleo que tiene el procesador instalado en el computador.
memory	Captura información de la memoria RAM instalada del computador, cantidad usada, disponible,
diskio	Captura información del espacio usado y espacio total de almacenamiento del disco duro del computador.
network	Captura información del uso de recursos del red del computador.
process	Datos de los procesos que se ejecutan en el computador, ejemplo uso de CPU, uso de memoria RAM que usa el proceso para ejecutarse
Process sumary	Datos del estado de los procesos en el computador.

Tabla 14. Descripción de parámetros de configuración del módulo system de *metricbeat*

Como segunda parte del caso 1 se implementa la captura de los datos Logs del servidor de VoIP con el elemento *filebeat* de *Elatic Stack*, inicialmente se instala *filebeat* dentro del servidor de VoIP (ver instalación en el anexo 1), terminada la instalación se configura la comunicación entre *filebeat* y *Elastic Cloud* (esta es la misma que se usó para *metricbeat* anteriormente), culminados estos dos procesos se configura la entrada de *filebeat* como input como se muestra en la Figura 15, para que tome los Logs que genera el servidor de VoIP y finalmente *filebeat* envía los logs para que se almacenen en *Elasticsearch.*

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/*.log
```

Figura 15. Configuración de entrada tipo Logs dentro de *filebeat*

En la Figura 15 se presenta la configuración de *filebeat*, en donde ***type*** es el tipo de entrada que va a recibir, ***enabled*** habilitar la entrada y ***paths*** es el lugar (carpeta dentro del sistema operativo Debian) donde se encuentran los logs, se coloca *.log para que tome todos los archivos que sean .log.

- **Caso 2:**

El switch Cisco SG500-52 52-port Gigabit Stackable es una fuente de datos donde el dispositivo de origen o que los contiene no se puede hacer uso *metricbeat* y *filebeat*, ya que

este dispositivo no cuenta con un sistema operativo como Windows, Linux o iOS, por lo tanto, para realizar la captura y recolección de datos, en el bloque A se configura el elemento *Logstash* de *Elastic Stack,* por medio de *Logstash* se capturan los datos de métricas de red y Logs generados por el switch mencionado.

Inicialmente antes de hacer la configuración de *Logstash*, se realiza la configuración en el switch Cisco SG500-52 52-port Gigabit Stackable para que pueda enviar datos por medio de SNMP, ya que *Logstash* requiere los parámetros que se muestran en la Tabla 15, para comunicarse con el switch, esta actividad es realizada por el ingeniero a cargo de la supervisión del proyecto dentro de la empresa como se detalla en el anexo 1.

Parámetro	Descripción
host	Dirección ip del dispositivo, puerto 161 Formato {tcp|udp}:{ip address}/{port}
community	Tipo de comunidad que usa puede ser pública o privada, Formato public o private
versión	Tipo de la versión 1, 2, 2c o 3

Tabla 15. Parámetros para la comunicación entre el Switch Cisco SG500-52 52-port Gigabit Stackable y servidor *Logstash*

Continuando con el proceso de configuración, se instala *Logstash* (ver anexo 1) en el servidor, llamado Servidor *Logstash*, que se dispuso en la empresa como se aprecia en la **Figura 6**, posteriormente se establece la comunicación entre *Logstash* y *Elastic Cloud*, para llevar a cabo esto se utilizan los parámetros de la Tabla 13. Luego para capturar los datos que contienen las métricas de red del switch Cisco SG500-52 52-port Gigabit Stackable, se utiliza el input SNMP de *Logstash* y dentro de input se agregan las OID [59] ver anexo 1, que son los objetos que contienen los datos de interés para este caso, en la Tabla 16 se muestran las OID que se usaron, posteriormente *Logstash* hace el envío de los datos para ser almacenados dentro de *Elasticsearch*.

En la misma figura, se observa que los datos capturados con el comando Tables vienen agrupados, debido a esto hay que usar el bloque B para procesar y poder separar la información, de esta manera trabajar con los datos individualmente.

OID	Nombre	Descripción	Comando dentro de *Logstash*
1.3.6.1.2.1.1.1.0	sysDescr	Descripción del dispositivo	Get
1.3.6.1.2.1.1.2.0	sysObjectID	Identificación autorizada por el proveedor	Get
1.3.6.1.2.1.1.5.0	sysName	Nombre asignado administrativamente es este dispositivo	Get
1.3.6.1.2.1.2.2.1.0	ifNumber	Numero de interfaces	Get
1.3.6.1.2.1.2.2.1.2	ifDescr	Tipo de interfaz de red	Tables
1.3.6.1.2.1.2.2.1.8	ifOperStatus	Estado de la interfaz de red	Tables
1.3.6.1.2.1.2.2.1.10	ifInOctets	Número total de octetos recibidos por la interfaz de red	Tables
1.3.6.1.2.1.2.2.1.11	ifInUcastPkts	Número de paquetes de unicast recibidos por la interfaz de red	Tables

1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts	Número de paquetes non-unicast recibidos por la interfaz de red	Tables
1.3.6.1.2.1.2.2.1.13	ifInDiscards	Número de paquetes entrantes que se eligieron descartarse	Tables
1.3.6.1.2.1.2.2.1.14	ifInErrors	Número de paquetes entrantes que contenían errores	Tables
1.3.6.1.2.1.2.2.1.16	ifOutOctets	Número total de octetos transmitidos por la interfaz de red	Tables
1.3.6.1.2.1.2.2.1.17	ifOutUcastPkts	Número de paquetes de unicast transmitidos por la interfaz de red	Tables
1.3.6.1.2.1.2.2.1.18	ifOutNUcastPkts	Número de paquetes non-unicast transmitidos por la interfaz de red	Tables
1.3.6.1.2.1.2.2.1.19	ifOutDiscards	Número de paquetes salientes que se eligieron descartarse	Tables
1.3.6.1.2.1.2.2.1.20	ifOutErrors	Número de paquetes salientes que contenían errores	Tables

Tabla 16. OID del Switch Cisco SG500-52 52-port Gigabit Stackable que contiene métricas de red

Como segunda parte de la implementación del caso 2 se requieren los datos Logs del switch Cisco SG500-52 52-port Gigabit Stackable; para cumplir con ello se emplea el elemento *Logstash,* y se configura el input como syslog, con este se debe tener en cuenta los siguiente: syslog usa por defecto el puerto 514 en algunos casos y para algunas empresas, ese puerto ya está en uso y se puede presentar conflicto, por tanto no llegan los datos a *Elastic Stack*, la solución es usar un puerto más alto el cual no esté en uso.

Teniendo en cuenta lo anterior se usa el puerto 62555 como se muestra en la Figura 16. Para ver la configuración completa ir al anexo 1.

Terminada la captura de datos Logs, se envían por *Logstash* para ser almacenados en *Elasticsearch*.

```
input {
  syslog{
    id => "psyslog"
    port => 62555
    type => syslog
    #codec => cef
    #syslog_field => "syslog"

  }
}
```

Figura 16. Parámetros de entrada para usar syslog con *Logstash*

4.2.2 Configuración de la adaptación del bloque procesamiento de datos

Para la configuración de la adaptación del bloque C se utiliza el elemento *Logstash*, dentro de las funcionalidades de este elemento se encuentra el transformar y modificar los datos, esto se logra por medio de los filtros, descritos en la Tabla 17. En la sección 4.2.1 se mostró

que unos datos necesitan una adecuación para su uso, los cuales se dividieron en tres casos.

Para desarrollar los casos presentados en la sección 4.2.1, se configura *Logstash* con los filtros descritos en la Tabla 17. La información detallada de la configuración se encuentra en el anexo 1.

Filtro	Función
Rename	Este filtro deja cambiar el nombre de los campos que contienen la información dentro de *Elasticsearch*. Se usa en conjunto con el filtro Mutate.
Ruby code	Enriquece un evento o campo con información que se desee agregar.
Mutate	Permite realizar una amplia variedad de cambios dentro de los campos de *Elasticsearch*, entre ellos se encuentran: cambio de nombre, eliminar información, y modificar campos.
Split	Es un filtro para dividir los campos agrupados dentro de una matriz o cadena en *Elasticsearch.*
Copy	Permite copiar un campo existente en otro campo. Se usa en conjunto Mutate.
Drop	Elimina todo lo que llega a este filtro.
Convert	Permite transformar y convertir el valor de un campo a un tipo diferente variable (entero, string, bool), por ejemplo, convertir una cadena en un número entero. Se usa en conjunto con Mutate.

Tabla 17. Filtros de *Logstash* para procesar datos

- **Caso 1:**

En la Figura 17 se muestran algunos datos obtenidos del switch Cisco SG500-52 52-port Gigabit Stackable. Como se aprecia en la imagen estos datos vienen con un campo de nombre extenso, lo cual dificulta el trabajo para la persona que necesita hacer uso de estos, por ello se usa el bloque B en donde se configura el filtro ***rename*** de *Logstash* para ajustar dicha longitud; después del filtro salen los datos ya procesados, se envían y almacenan dentro de *Elasticsearch*.

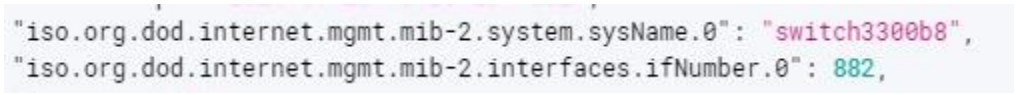

Figura 17. Datos no procesados de capturado por el bloque A

- **Caso 2:**

En la sección 2.2.2.2.3 se manifestó que se necesita ver la cantidad de paquetes entrantes y salientes, para ello se emplean las ecuaciones 1 y 2, las cuales se configuran dentro del bloque B con uso del filtro ***ruby*** y ***code*** del elemento Logstash, esto permite hacer la operación suma de los campos *unicast* con *non-unicast* que contienen estos datos, tal como

se muestra en la Figura 18, el resultado se envía a *Elasticsearch* y se almacena en los campos *inpacket* y *outpacket*.

$$inpacket = inpacketunicast + inpacketnonunicast \quad (1)$$

$$outpacket = outpacketunicast + outpacketnonunicast \quad (2)$$

```
ruby {
        code => "
        event.set('network.in.packets', event.get('[interface][in][uni][pack]').to_i + event.get('[interface][in][non][pack]').to_i )
        event.set('network.out.packets', event.get('[interface][out][uni][pack]').to_i + event.get('[interface][out][non][pack]').to_i )
        "
    }
```

Figura 18. Suma de cantidad de paquetes *unicast* con los *non-unicast* entrantes y salientes

- **Caso 3:**

Para terminar, se describe la implementación del cambio de tipo de dato, ya que se está presentando la siguiente situación en *Logstash*, previamente se implementó la captura del estado de las interfaces físicas del switch Cisco SG500-52 52-port Gigabit Stackable por medio de las OID, al ingresar los datos estos quedan como dato entero, para solventar esto se implementó el filtro ***mutate***, ***copy*** dentro de *Logstash* y se termina con ***add_field***, con esto, la salida de los datos queda en tipo *string* el cual es el formato que se necesita, para ver la configuración dirigirse al anexo 1.

4.2.3 Configuración de la adaptación del bloque visualización datos

En la sección 4.1, se indica que se tiene acceso a todas las funciones de *Elastic Stack* con el entorno de operación; gracias esto la configuración de la adaptación del bloque C se realiza con la función ***Visualize*** del elemento *Kibana* que es parte de *Elastic Stack*.

La función *Visualize* ofrece una gran variedad de plantillas para crear visualizaciones con los datos como se muestra en la Figura 19 y su descripción en la Tabla 18. A continuación se listan las opciones de visualización a recrear para tener una imagen completa de los equipos sobre los cuales se están realizando las mediciones.

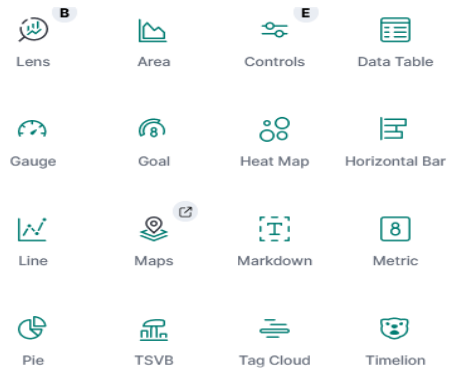

Figura 19. Tipos de visualizaciones en la sección *visualize*

Tipo de visualización	Uso
Gauge	Representa el estado de una métrica, se usa para mostrar cómo se relaciona un valor de un variable con un valor umbral.
TSVB(*Time Serial Visualization*)	Representa la información de múltiples series de datos, permite realiza operaciones básicas (suma, resta) Para usar este tipo de visualización los datos debe contener el campo fecha .
Bar vertical/horizontal	Representa la información en forma de barra, se puede mostrar de forma vertical u horizontal.
Pie	Representa la información en forma de torta o dona.
Data table	Representación de datos en forma de tabla
Controls	Permite controlar acciones y navegar dentro las visualizaciones.
Heap Map	Muestra la información en forma de matriz
Metric	Representa el valor de una única métrica numérica especifica.

Tabla 18. Descripción de las opciones de visualización en la sección *visualize*

Las visualizaciones, se dividen en dos grupos, una para los datos del servidor de VoIP y la otra para el switch Cisco SG500-52 52-port Gigabit Stackable, las cuales se muestran en las tablas 19 y 20 respectivamente.

NÚMERO	VISUALIZACIÓN	UNIDAD EXPRESADA/TIPO DE DATO
1	Consumo de CPU	Porcentaje
2	Consumo de memoria RAM	Porcentaje
3	Disco duro usado	Byte
4	Cantidad de procesos.	Entero
5	Consumo de memoria RAM usada vs instalada.	Byte
6	Cantidad de disco duro usado vs instalado	Byte
7	Tráfico de red entrante y saliente de la tarjeta de red.	Mbps, Kbps, bps
8	Consumo de CPU de cada proceso ejecutado.	Porcentaje
9	Consumo de memoria RAM de cada proceso ejecutado.	Porcentaje
10	Logs generados por el servidor de VoIP	String (cadena)

Tabla 19. Visualización para los datos del servidor de VoIP

NÚMERO	VISUALIZACIÓN	UNIDAD EXPRESADA/TIPO DE DATO
11	Información básica (nombre del Switch	String (cadena)
12	Estado de cada uno de los puertos físicos (UP/DOWN)	String (cadena)

13	Cantidad de puertos que presentan estado UP y DOWN	Entero
14	Cantidad de tráfico de red entrante de cada una de los puertos físicos	Mbps, Kbps, bps
15	Cantidad de tráfico de red saliente de cada uno de los puertos físicos.	Mbps, Kbps, bps
16	Cantidad de paquetes entrantes en cada puerto físico.	Entero
17	Cantidad de paquetes salientes en cada puerto físico.	Entero
18	Cantidad de paquetes entrantes descartados en cada puerto físico.	Entero
19	Cantidad de paquetes salientes descartados en cada puerto físico.	Entero
20	Cantidad de paquetes entrantes con errores en cada puerto físico.	Entero
21	Cantidad de paquetes salientes con errores en cada puerto físico.	Entero
22	Logs generados por el switch Cisco SG500-52 52-port Gigabit Stackable	Entero

Tabla 20. Visualizaciones para el Switch Cisco SG500-52 52-port Gigabit Stackable

Dentro del proceso de creación de las visualizaciones, la primera consideración es tener claro cómo se desea mostrar y representar la información para el usuario final.

Para la realización de las visualizaciones de la Tabla 19 cuya unidad para mostrar será un porcentaje, se usó la plantilla ***Gauge***, como se muestra en la Figura 20.

Figura 20. Visualizaciones de datos expresados en porcentaje

Para visualizaciones cuya unidad será en Byte y cantidad de procesos, estas se crean por medio de ***metric***, ya que solo es de interés mostrar un solo valor (cantidad de procesos activos, consumo de memoria RAM y almacenamiento usada vs instalado), como se presenta en la Figura 21.

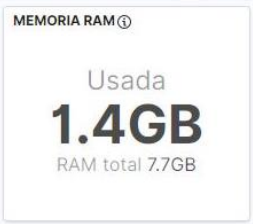

Figura 21. Visualización de cantidad memoria RAM

Para la visualización que requieren de operaciones numéricas como suma, resta, multiplicación, división, se realizan con ***TSVB*** ya permite el uso de barras verticales y horizontales, además de ofrecer en cambio de formato en unidades como Byte, porcentaje, bool entre otras, las barras verticales se usan para la visualización número 7 (en la visualización se emplean las unidades Gibit/s, Mibit/s, Kibit/s, bit/s ya que la herramienta no tiene el formato de Gbps, Mbps, Kbps y bps). Para las visualizaciones número 8 y 9 se emplean barras horizontales para que el usuario observe como va creciendo o disminuyendo el de uso de recursos usados expresados en porcentaje, como se aprecia en la Figura 22.

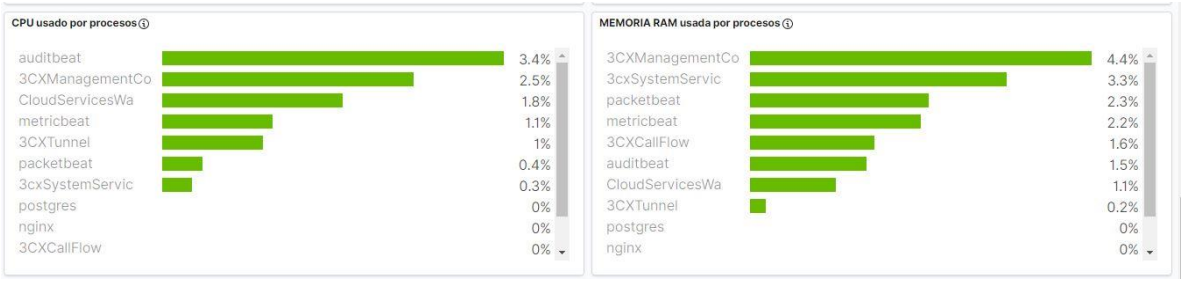

Figura 22. Visualizaciones número 8 y 9 mostrando datos expresados en porcentaje

Por último, se crea la visualización número 10, cuya información está en formato de cadena; por ello, se hace uso de la visualización ***Data Table***, esta se puede observar en la Figura 23.

Figura 23. Visualización 10 datos de Logs presentados en forma de tabla

Con lo anterior terminan todas las visualizaciones realizadas para el servidor de VoIP. La creación de todas las anteriores se presenta en el anexo 1.

En la segunda parte de esta sección se realizan las visualizaciones para el switch Cisco SG500-52 52-port Gigabit Stackable. Se inicia con la creación de la visualización número 11, para la cual se emplea el tipo ***Data Table***; aquí, se añaden los datos del nombre del switch y la cantidad de interfaces que este tiene, como se muestra en la Figura 24,

Figura 24. Visualización con datos de la información básica del switch Cisco SG500-52 52-port Gigabit Stackable

Para la visualización número 12, el tipo ***Heap Map*** es más adecuado para presentar los datos del estado de las interfaces físicas, esta permitió ver los datos de los nombres de las interfaces, y adicionar un color para identificar el estado de cada una de ellas, de la siguiente manera: color rojo para las que tiene estado DOWN y color verde para que tienen estado UP, como se puede ver en la Figura 25.

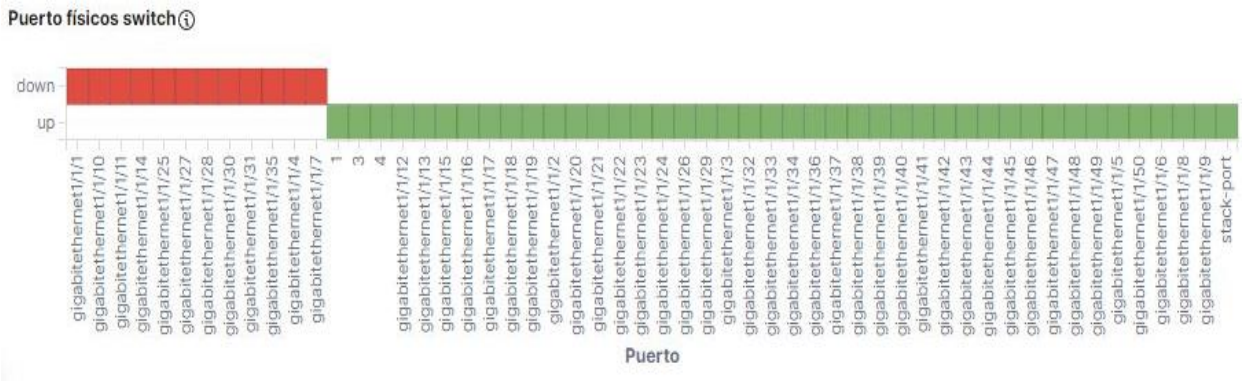

Figura 25. Visualización del estado de cada uno de los puertos físicos del switch Cisco SG500-52 52-port Gigabit Stackable

Para la visualización número 13 se emplea ***metric*** ya que aquí se necesita ver solo un valor numérico que corresponde al conteo de la cantidad de puertos físicos en estado UP y DOWN como se aprecia en la Figura 26.

Figura 26. Visualización del conteo de la cantidad de puertos que presentan estado UP y DOWN en el switch Cisco SG500-52 52-port Gigabit Stackable

Para las visualizaciones, ya para las visualizaciones número 14, 15, 16, 17, 18, 19, 20 y 21 se emplea ***TSVB*** para presentar los datos en forma de barras y porque permite realizar operaciones como sumar, restar, multiplicar, dividir con los datos que se están usando dentro de la visualización, como se aprecia en la Figura 27.

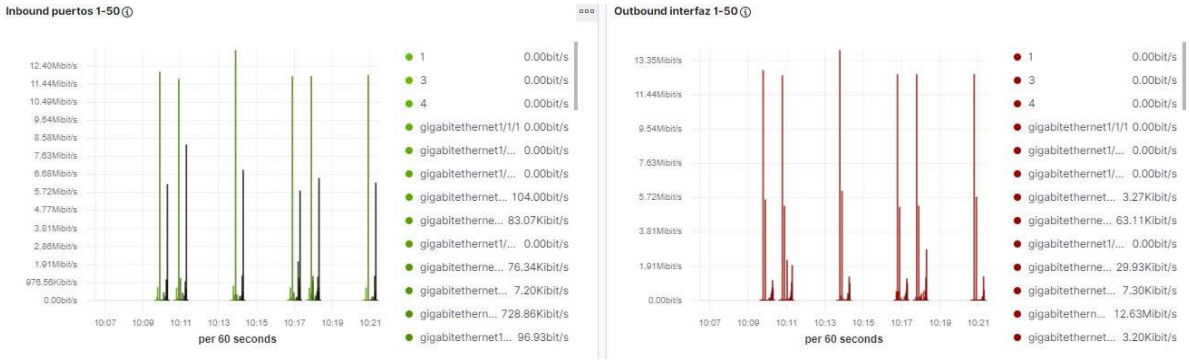

Figura 27. Visualización de la cantidad de tráfico de red entrante y saliente de cada una de los puertos físicas en el switch Cisco SG500-52 52-port Gigabit Stackable

Por último, se requiere presentar los datos de los Logs del switch Cisco SG500-52 52-port Gigabit Stackable, para este caso particular se utiliza una búsqueda de la sección ***Discover*** y se almacena, esto permite navegar y hacer búsqueda de palabras claves dentro de los datos Logs. La Figura 28, representa lo descrito.

Figura 28. Visualización de los datos de Logs del switch Cisco SG500-52 52-port Gigabit Stackable

Toda la información de la creación de las anteriores visualizaciones se encuentra en el anexo 1.

4.2.4 Configuración de la adaptación del bloque *Machine Learning*

El bloque D se pone en funcionamiento con la función de ***Machine Learning*** que se encuentra dentro de *Kibana*. Antes de realizar la implementación se introducirán los conceptos de unos parámetros clave que se van a usar dentro de esta función, los parámetros son: ***job*** (trabajo), ***datafeed*** (fuente de datos), ***detector***, ***influencer***. El parámetro denominado *job* es el que se encarga de hacer el análisis de los datos de interés, permite analizar un dato en particular denominado ***single metric*** o varios datos simultáneamente denominado ***multi-metric*** para realizar una correlación de estos. El *datafeed*, son los datos que se desea analizar, el *detector* se usa para definir el tipo de análisis a realizar, algunas de estas son: max, average, rare, min entre otras, por ejemplo,

el detector ***max*** identifica el valor máximo que se encuentra en los datos suministrados y el *influencer* es uno o máximo tres datos que se suministran dentro del *job*, de los cuales el usuario tiene sospechas que contienen información acerca de algo que influye en anomalías en sus datos.

Ahora, se procede a realizar la configuración de los parámetros de *Machine Learning*. Inicialmente se crea un *job* y se añaden los datos de interés, a continuación, se ingresan los *detectors* y los *influencer* para que con estos dos parámetros se realice el respectivo análisis de los datos. Terminado el análisis de los datos, este arroja los resultados como se muestra en la Figura 29, en la figura se identifican una matriz llamada ***overall*** y top ***influencer*** con una numeración.

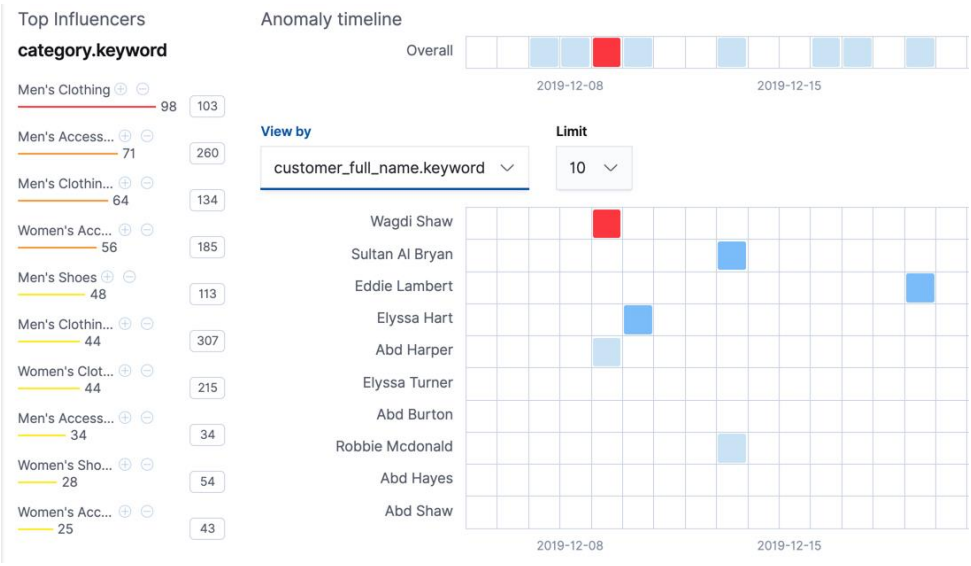

Figura 29. Resultado del estudio de *Machine Learning*

La matriz *overall* muestra con un color a la detección de un dato anómalo que pertenece a datos suministrados, este dato anómalo se detectó con respecto a los *detectors* e *influencer* configurados previamente, el valor numérico adjunto a los datos debajo de ***Top influencer*** representan el nivel se severidad o gravedad, los niveles de severidad se muestran en la Tabla 21, estos indican que tan grave es el dato anómalo que encontró el estudio respecto a los datos que se le suministraron.

Nivel de severidad	Rango	Color
Warning (advertencia)	0-24	Blanco
Minor (menor)	25-49	Amarillo
Major (importante)	50-74	Naranja
Critical (crítico)	75-100	Rojo

Tabla 21. Niveles de severidad para clasificar un evento anómalo con *Machine Learning*

4.2.5 Configuración de la adaptación del bloque alertas

Para la configuración de la adaptación del bloque E, alertas, se realizan dos procesos, el primero es para los datos del servidor de VoIP en la cual se emplea la función ***Alert and Actions*** que se encuentra en el elemento *Kibana*, y la segunda para el switch Cisco SG500-

52 52-port Gigabit Stackable que se configura dentro de las visualizaciones creadas en la sección 4.2.3.

Inicialmente se configuran las alertas para el servidor de VoIP, estas se crean por medio ***Alert and Actions***, en donde se parametrizan los siguientes datos: nombre de la alerta, nombre del dato que se desea supervisar o vigilar, condición (Qué hay que detectar), programación (cuándo y con qué frecuencia se realiza la comprobación de la detección) y acciones. Primero se crea el nombre de la alerta y la programación de cada cuánto tiempo se revisa la condición, la programación se puede configurar en días, horas, minutos o segundos como se muestra en la Figura 30.

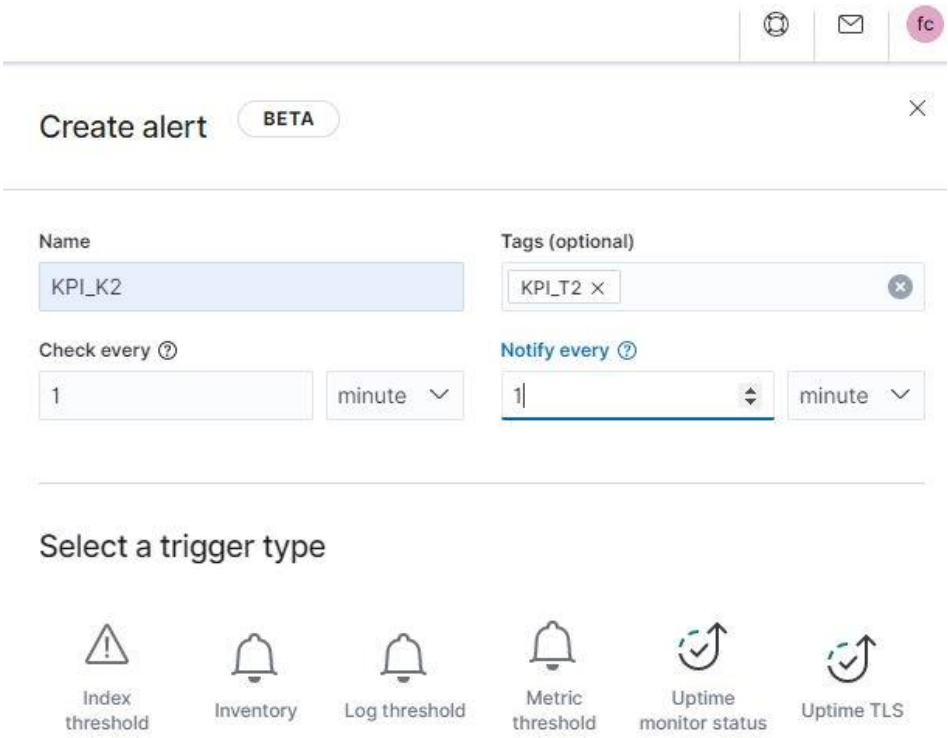

Figura 30. Parámetros para la creación de una alerta

Terminadas estas configuraciones se establece la condición con la cual se va activar la alerta, la cual puede ser: cuando el promedio sea menor que, cuando el promedio sea mayor que, cuando la suma sea mayor que, entre otras, seguido del nombre del dato que se va a supervisar, en la Figura 31 se aprecia un ejemplo.

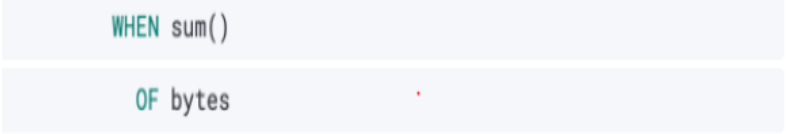

Figura 31. Parámetro de condición para creación de una alerta

Finalmente se selecciona el conector (es donde se envía la alerta al usuario) ***connector***, los cuales pueden ser Email, PagerDuty, Slack o Webhook. Los conectores se muestran en la Figura 32, para este caso de uso se utilizó el conector Slack, la configuración y la creación de la cuenta se muestra en el anexo 1.

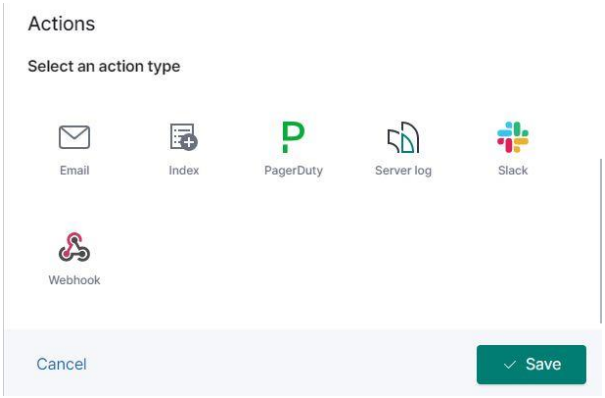

Figura 32. Conectores de las alertas dentro de *Kibana*

Dentro de la segunda parte que corresponde a la configuración de las alertas para el switch Cisco SG500-52 52-port Gigabit Stackable, estas se crean directamente en las visualizaciones, ya que al haber usado TSVB, este permite hacer operaciones y crear niveles estáticos los cuales se toman como los valores de referencia para los *targets* y *threshold*.

5. CAPÍTULO V. Evaluación de la herramienta adaptada *Elastic Stack*

En esta sección presenta las pruebas para verificar que la herramienta se adaptó adecuadamente para medir el desempeño del servicio de VoIP.

Las pruebas realizadas sobre la infraestructura definida anteriormente, consistieron en lo siguiente:

1. Capturar datos en tiempo real el uso de recursos de capacidad (CPU, memoria RAM, disco duro, entre otros) del servidor VoIP y almacenarlos dentro de *Elasticsearch*.
2. Crear visualización con los datos del servidor VoIP dentro de *Elasticsearch*.
3. Crear alertas y enviar al usuario del área de trabajo.
4. Capturar los datos de red del switch Cisco SG500-52 52-port Gigabit Stackable por medio SNMP.
5. Procesar datos del switch Cisco SG500-52 52-port Gigabit Stackable.
6. Capturar datos de Logs del switch Cisco SG500-52 52-port Gigabit Stackable por syslog.
7. Crear visualización con los datos del switch Cisco SG500-52 52-port Gigabit Stackable.

- Prueba 1: Capturar datos en tiempo real del uso de recursos de capacidad del servidor de VoIP

Esta prueba consiste en verificar que los datos se están capturando de la fuente y se están enviando a *Elasticsearch* en la nube en tiempo real. Cuando los datos son capturados y llegan correctamente a *Elasticsearch,* primero este crea índices con el nombre del *beat* que se está usando, en la parte ***Storage size*** se ve el tamaño de la información acumulada expresada en ***Byte***, si el valor en ***Storage size*** es cero, significa que no se está almacenado información en el índice; para este caso el *beat* empleando es *metricbeat* y se puede observar que se ha creado un índice con el nombre de *metricbeat* y en ***Storage size*** el valor es diferente de cero como se aprecia en la Figura 33. Posteriormente los datos los puede ver y leer por usuario en la sección ***Discover*** de *Kibana* como se muestra en la Figura 34.

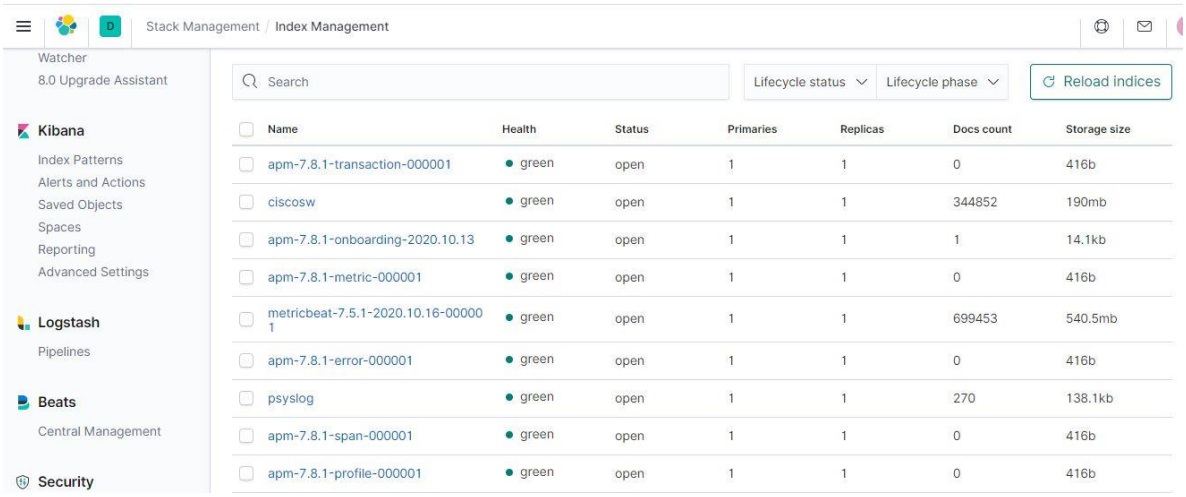

Figura 33. Verificación de datos dentro de *Elasticsearch*

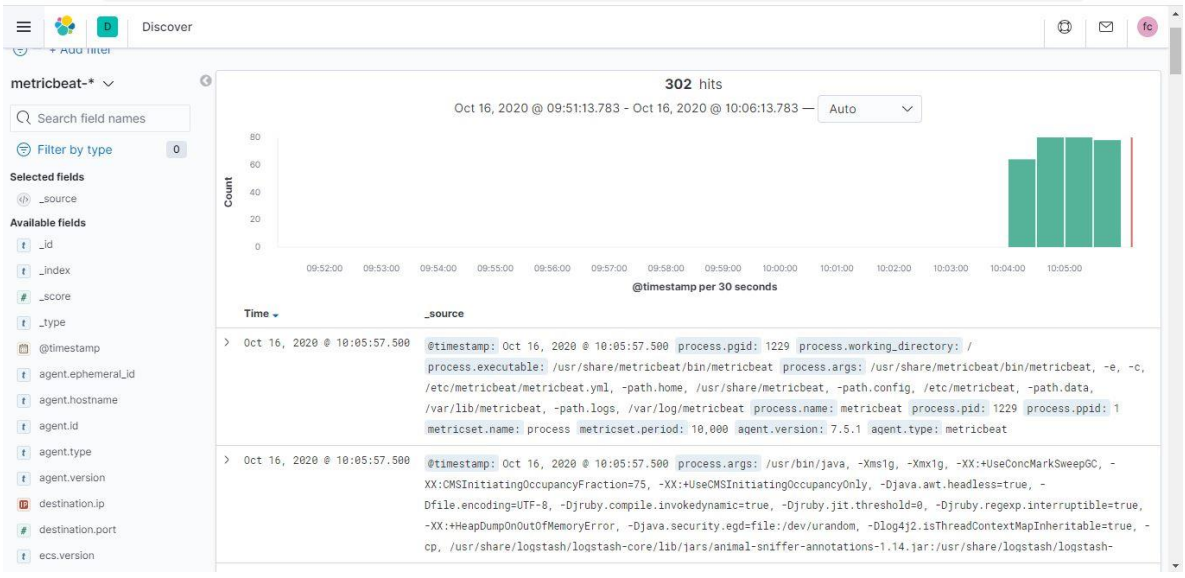

Figura 34. Datos dentro de *Elasticsearch* visto en la sección Discover

- Prueba 2: Crear visualización con los datos dentro de *Elasticsearch*

Para esta prueba se usan los datos que están almacenados en *Elasticsearch,* con ellos se realizan las visualizaciones por medio de la función ***Visualize***, en la cual se selección una plantilla y se añade los datos que desean mostrar al usuario, para este caso tenemos la plantilla ***Gauge*** que muestra en consumo de CPU y lo expresa en porcentaje como se aprecia en la Figura 35.

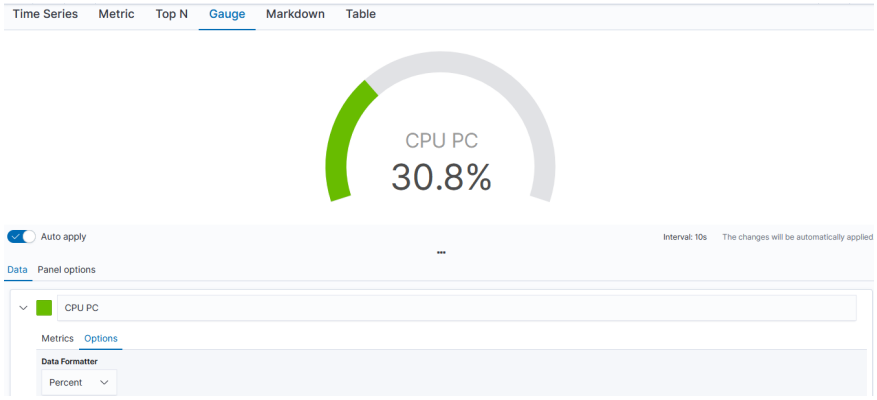

Figura 35. Visualización con los datos de CPU del servidor de VoIP

- Prueba 3: Crear alertas y enviar al usuario del área de trabajo

En esta prueba se crea una alerta con la función ***Alert and Actions***. Primero se crea el nombre de la alerta como KPI, el *tag "*server" para identificar que esta alarma viene del servidor de VoIP, con la condición de que active cuando el valor de system.cpu.total.pct este por encima del 2% (0.02), con tiempo de verificación cada 1 minuto y conector Slack.

Posteriormente, se crean las variables de acción, estas son datos que se muestran en conjunto cuando la alerta se activa, por ejemplo: la fecha en que se generó la alerta, el valor con el cual se está comparando la alerta, el valor que hizo activar la alerta, entre otros, esta configuración se aprecia en la Figura 36.

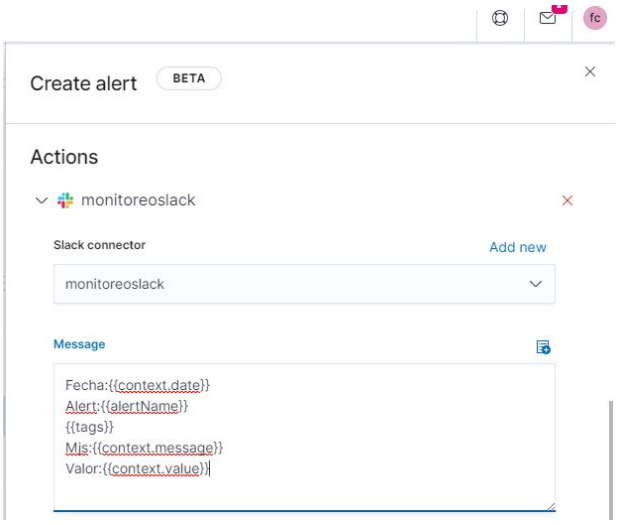

Figura 36. Configuración de datos que ve el usuario dentro de la alerta creada

Finalmente se guarda y queda activa la alerta para que corrobore que, si se ha excedido el valor configurado, en cuyo caso deberá mandar un mensaje a Slack con el nombre del dato que presento esta situación, valor con el cual se superó el nivel establecido. Esto se aprecia en la Figura 37.

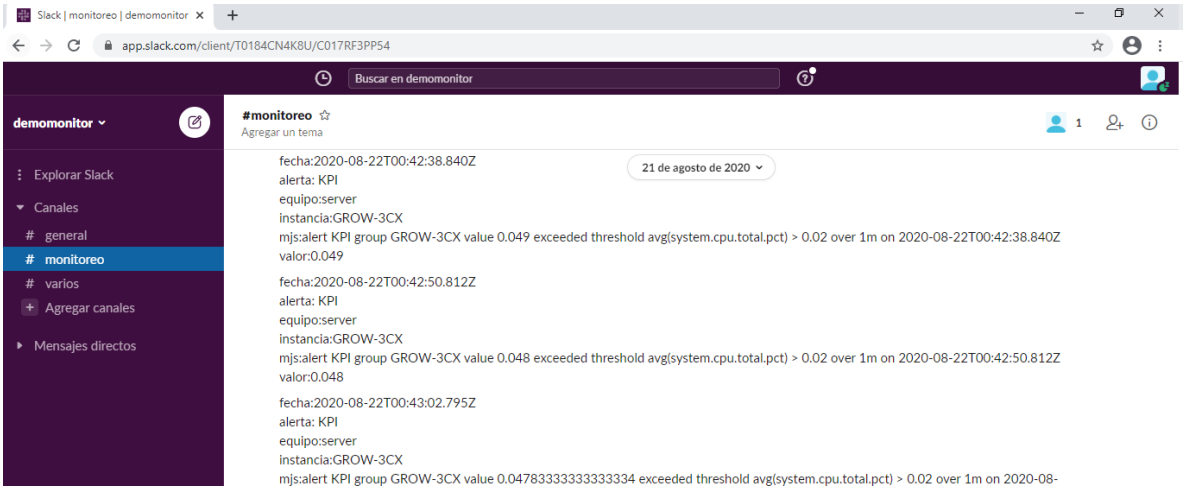

Figura 37. Alerta que recibe el usuario final y la visualiza dentro de Slack

- Prueba 4: Capturar los datos de red del switch Cisco SG500-52 52-port Gigabit Stackable por medio SNMP

Esta prueba permite verificar que se está capturando los datos del switch Cisco SG500-52 52-port Gigabit Stackable por medio de SNMP. Primero se captura la información empleando ***MIB Browser*** de *iReasoning,* esta herramienta permite cargar MIB y emitir solicitudes SNMP para recuperar los datos de los agentes SNMP como se aprecia en la Figura 34 y luego se hace el proceso de captura con *Logstash*, y luego se almacena lo datos dentro *Elasticsearch* como se aprecia en la Figura 38. Al comparar la Figura 38 y 39 se observa que sysDescr.0 tiene el mismo dato “52-Port Gigabit Stackable Maneged Switch”.

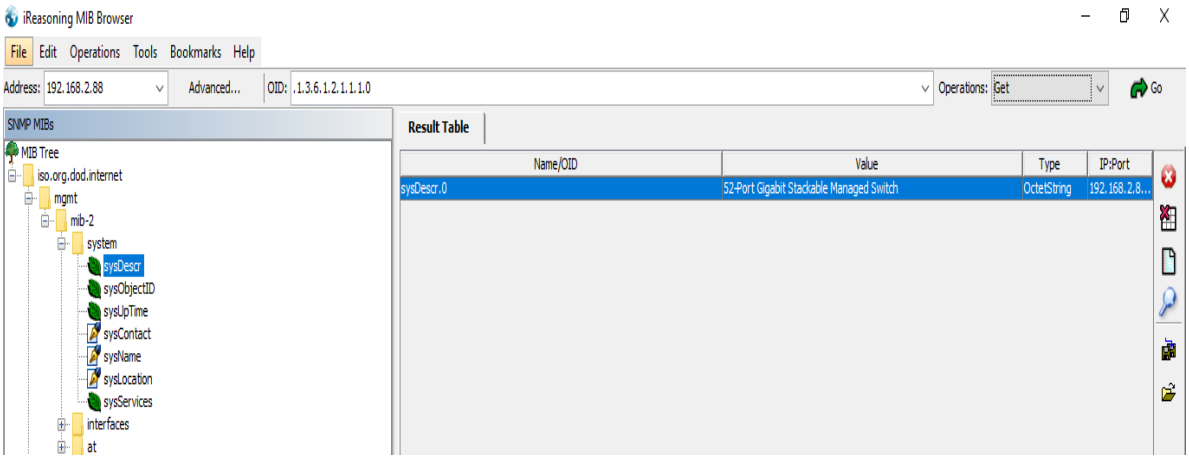

Figura 38. Datos tomados con la herramienta MIB Browser de iReasoning

Figura 39. Datos capturados con *Logstash* por medio de SNMP

- Prueba 5: Procesar datos del switch Cisco SG500-52 52-port Gigabit Stackable por medio SNMP.

Esta prueba consiste en procesar datos para poderlos usar; algunos de ellos datos están almacenados en campos con nombres extensos, para usarlos de manera más eficiente por el usuario se debe cambiar esta extensión por una más corta, esto lo hace el filtro *rename* de *Logstash*; la información entra al filtro con el nombre largo y sale con el nombre corto como se aprecia en la Figura 40 y 41 respectivamente.

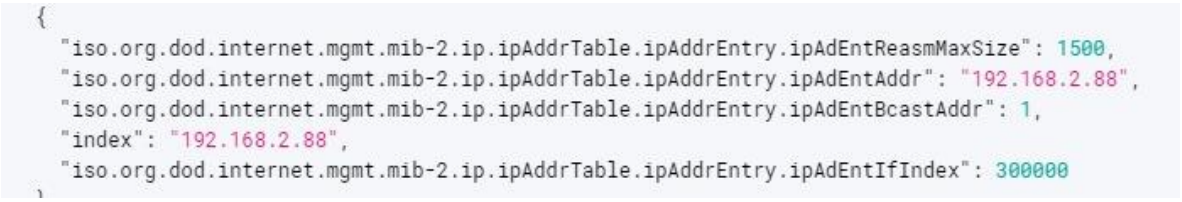

Figura 40. Datos sin procesar con nombre largo

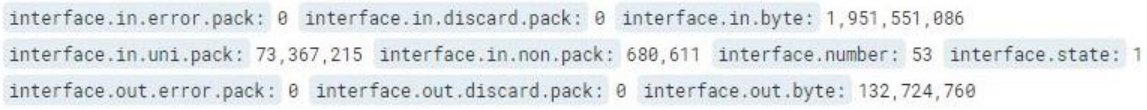

Figura 41. Datos procesados con nombre corto

- Prueba 6: Capturar datos de Logs del switch Cisco SG500-52 52-port Gigabit Stackable por medio syslog

Esta prueba permite verificar que se están capturando los datos Logs del switch Cisco SG500-52 52-port Gigabit Stackable por medio de syslog de *Logstash*, para ello primero se verifica que se haya creado el índice dentro de *Elasticsearch*, como los datos se toman con *Logstash*, este permite definir el nombre del índice donde se almacena estos datos, el cual se le coloca el nombre de **psyslog**, en la parte derecha del nombre se ve como Storage size tiene un valor de 138 KB lo que indica que se está llenando de datos como se muestra en la Figura 42, una vez se verifica que los datos si están almacenados dentro de *Elasticsearch*, estos se pueden apreciar dentro de *Discover* como lo indica la Figura 43.

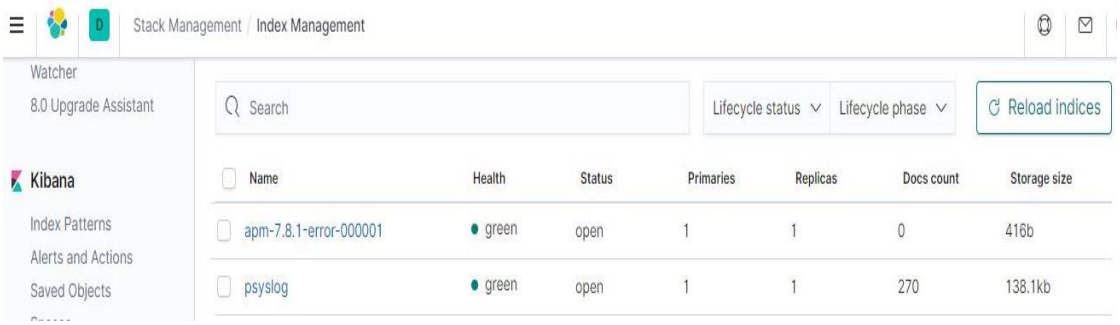

Figura 42. Logs del switch Cisco SG500-52 52-port Gigabit Stackable almacenados dentro del *Elasticsearch*

Figura 43. Captura de Logs del switch Cisco SG500-52 52-port Gigabit Stackable almacenados en Elasticsearch

- Crear visualización con los datos del switch Cisco SG500-52 52-port Gigabit Stackable

Esta prueba consiste en mostrar los datos capturados del switch Cisco SG500-52 52-port Gigabit Stackable en un panel de visualización al usuario final, para ello se toman los datos que se encuentran en el índice ciscosw y se añaden a la visualización el resultado final es la Figura 44.

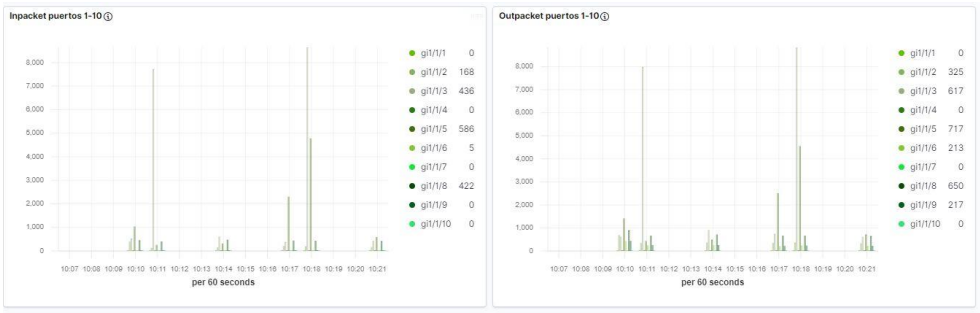

Figura 44. Visualización de la cantidad de paquetes entrantes y salientes en cada puerto del switch Cisco SG500-52 52-port Gigabit Stackable

Concluidas las pruebas de funcionamiento de la herramienta *Elastic Stack* se procede a realizar los dashboard con las visualizaciones creadas y luego a realizar la medición de los servicios TI por medio de KPI con el uso de las alertas y el estudio de *Machine Learning.*

Ya terminadas las visualizaciones, estas se incluyen dentro de dos dashboard, el primero contiene todas las visualizaciones del servidor de VoIP y el segundo las visualizaciones switch Cisco SG500-52 52-port Gigabit Stackable, llamados “PC Datos” y “switchcisco” respectivamente, adicionalmente estos se introducen en un dashboard llamado presentación para ofrecer al usuario un menú más amigable. En las Figuras 45, 46, 47 se observan los dashboard mencionados anteriormente.

Figura 45. Dashboard de presentación

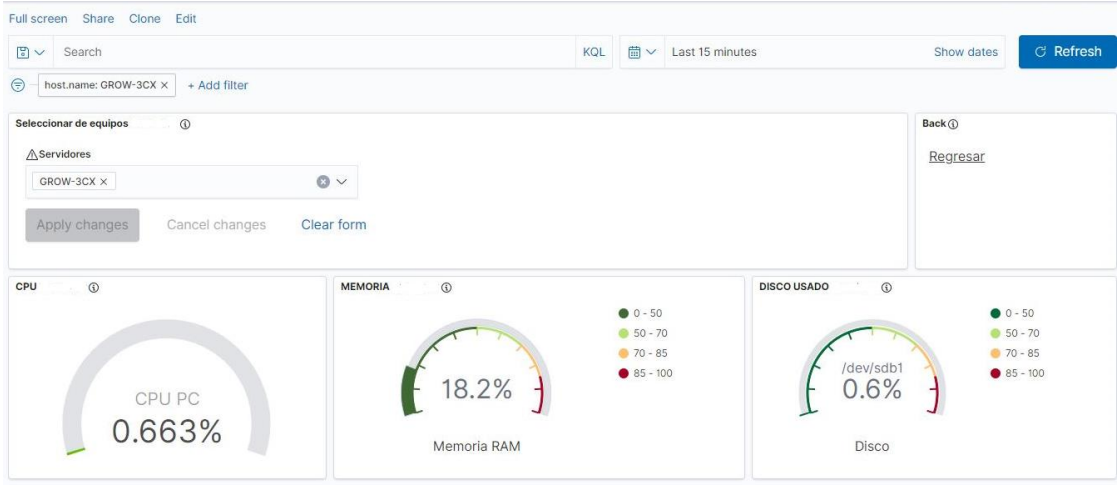

Figura 46. Dashboard con información del servidor de VoIP

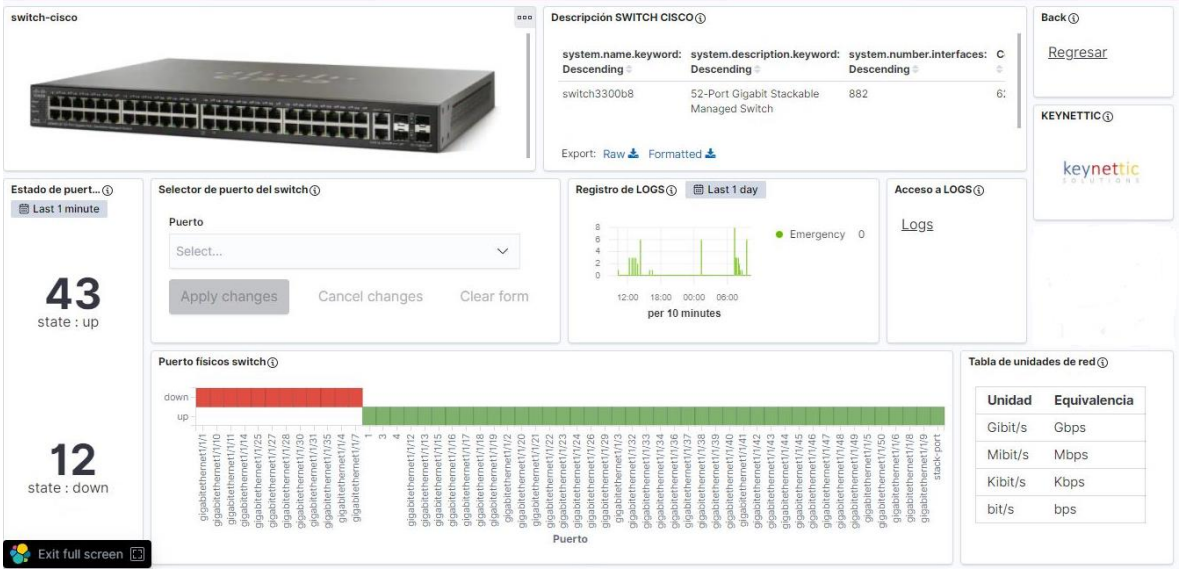

Figura 47. Dashboard del switch Cisco SG500-52 52-port Gigabit Stackable

Con la herramienta adaptada se procede a realizar la medición del desempeño de servicios por medio de los KPI planteados con las siguientes actividades:

1. Crear alertas para supervisar los KPI formulados para el servidor de VoIP.
2. Realizar análisis de datos de consumo de CPU y memoria RAM del servidor de VoIP por medio de *Machine Learning.*
3. Fijar límites de consumo dentro de las visualizaciones y supervisar los KPI del switch Cisco SG500-52 52-port Gigabit Stackable.

- Crear alertas para los KPI formulados

En la Tabla 5 de la sección 2.2.2.1.3 se presentaron los KPI ***K1*** y ***K2*** que se deben supervisar, teniendo en cuenta estos valores se procede a realizar las alertas.

Dentro de *Elasticsearch* la alerta que se relaciona con uso de CPU se denomina como ***KPI_K1,*** esta alerta se activará cuando “system.cpu.user.pct” (consumo de CPU en porcentaje) esté por encima o igual a 50% (0.5), y se agrupara por “process.name” para conocer qué proceso activó la alerta, la verificación se establece para los últimos 5 minutos pasados, la configuración se muestra en la Figura 48. El proceso anterior se repite para la configuración de ***KPI K2****.*

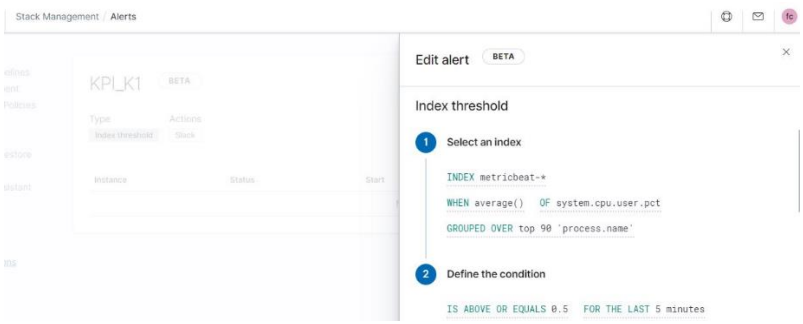

Figura 48. Configuración de la alerta para KPI_K1

Después se configuradas las alertas, se guardan y se activan para que comience la supervisión de los KPI, si la alarma es activada se enviará un mensaje hacia Slack.

- Realizar análisis de datos de consumo de CPU y memoria RAM del switch Cisco SG500-52 52-port Gigabit Stackable por medio de *Machine Learning.*

Se crea un *job* de *Machine Learning* tipo *multi-metric* para analizar los datos en el consumo de CPU y memoria RAM. Después se añaden los *datafeed* para este caso son los datos de CPU y memoria RAM que se encuentran almacenados dentro de *Elasticsearch*, con el *detector max* para detectar el valor máximo y *high mean* para encontrar valores por encima de la media, por último, el *influencer* process.name para identificar qué proceso es el que presenta la anomalía en sus datos.

- Fijar límites de consumo dentro de las visualizaciones y supervisar los KPI del switch Cisco SG500-52 52-port Gigabit Stackable

Dentro las visualizaciones creadas que contienen datos de red del switch Cisco SG500-52 52-port Gigabit Stackable se establecen los limites (valores estáticos), estos valores representan los KPI de la Tabla 3 sección 2.2.2.2.3. En la Figura 49 se presenta la gráfica de tráfico entrante para la interfaz gigabitethernet1/1/12 en la cual se añadió los valores de prueba de *T3 (target)* igual a 3.81 Mbps y el valor de M3 (*Threshold*) igual a 4.7 Mbps, de esta manera poder ver gráficamente en qué momento los datos están en valores normales o cuando se están sobrepasando.

Figura 49. Visualización de prueba para supervisar los valores de tráfico entrante de la interfaz gigabitethernet1/1/12.

- Resultados de las alertas para supervisar los KPI formulados para el servidor de VoIP

Analizando las alertas almacenadas dentro de Slack, se aprecia que no se han activado ninguna para el KPI formulado, solo están las alertas que se generaron para hacer las pruebas de funcionamiento, esto quiere decir que, las los KPI para consumo de CPU y memoria RAM no superaron el valor de los *Target* establecidos durante toda la toma de datos como se aprecia en la Figura 50.

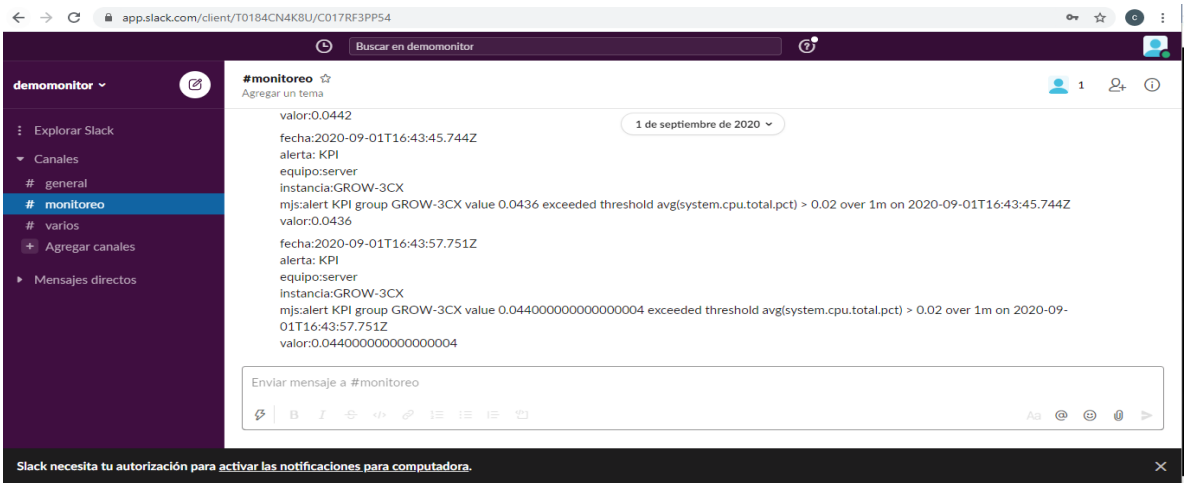

Figura 50. Reporte de alertas dentro de Slack para KPI K1 y K2

- Resultados análisis de datos de consumo de CPU y memoria RAM del servidor de VoIP por medio de *Machine Learning.*

El *job* de *Machine Learninig* arrojó los resultados del análisis de los datos de consumo de CPU y memoria RAM que se muestran en la Figura 51 y 52. En la Figura 51 se presenta la ocurrencia de datos anómalos, los cuales se representan por la matriz *overall*, además también se presenta bajo el aparte de *Anomalies* información específica sobre las ultimas anomalías encontradas.

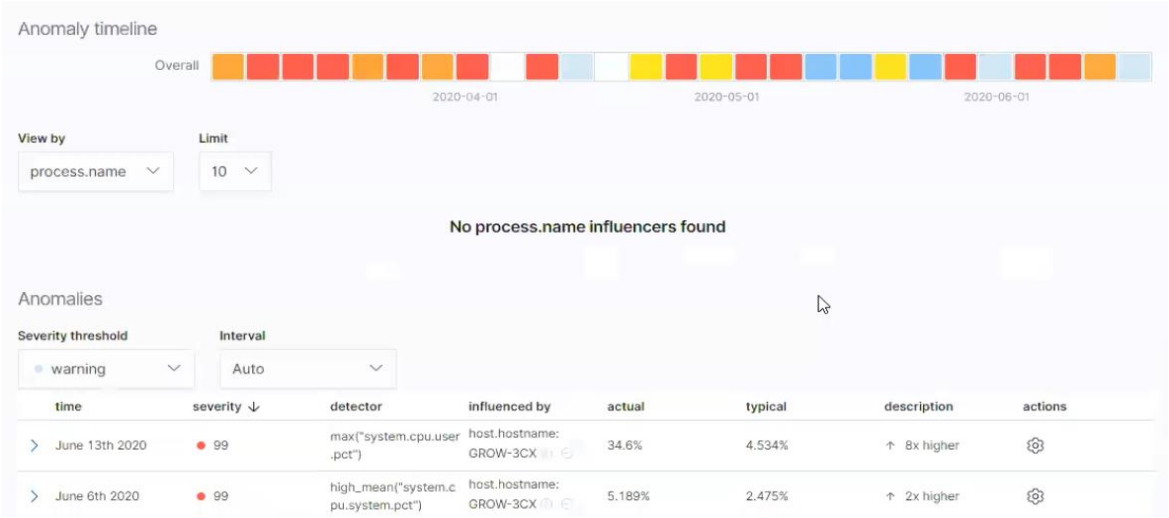

Figura 51. Resultados del análisis de datos de consumo de CPU y memoria RAM con *Machine Learning*

El día 13 de junio de 2020 se detectó una anomalía, ya que el consumo típico de CPU es de 4.53% y ese día el uso de CPU subió al 34.6%, a este evento se le asignó una severidad de 99 dado que se está usando 8 veces más recursos que el consumo típico, adicional a esta información se muestra en el resultado la hora en que sucedió el evento (entre 13:45 y 14:00), el equipo afectado (nombre host) y la probabilidad de que este evento ocurra, como se describe en la Figura 52.

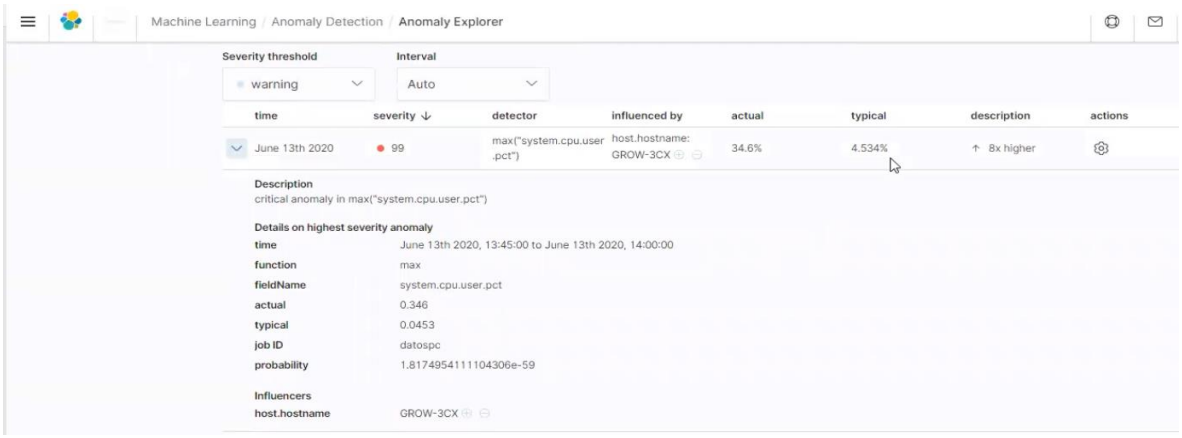

Figura 52. Datos detallados de una anomalía del 13 de junio de 2020

Este resultado permite confirmar el correcto funcionamiento de las alarmas ya que no se detectaron valores de consumo superiores al 50 % y por lo tanto no se generó ninguna alarma.

- Resultados de la supervisión de los KPI (tráfico entrante y saliente) del switch Cisco SG500-52 52-port Gigabit Stackable

A continuación, se analizan las mediciones de tráfico entrante y saliente en las interfaces del switch. Para simplificar este proceso, se muestran las gráficas asociadas a una sola interfaz, sin embargo, la herramienta permite visualizar de manera independiente cada una de sus interfaces activas. Como se observa en la Figura 25, las interfaces del switch están configuradas a una velocidad máxima de 1Gbps, por lo tanto, los limites tendrán los siguientes valores; *T3*=500Mbps y *M3*=800Mbps. Sin embargo, como se aprecia en la Figura 27 el consumo máximo para las interfaces no supera los 12.40 Mbps, este valor se encuentra considerablemente por debajo de los umbrales *T3* y *M3* y se representa por la línea verde en la Figura 53.

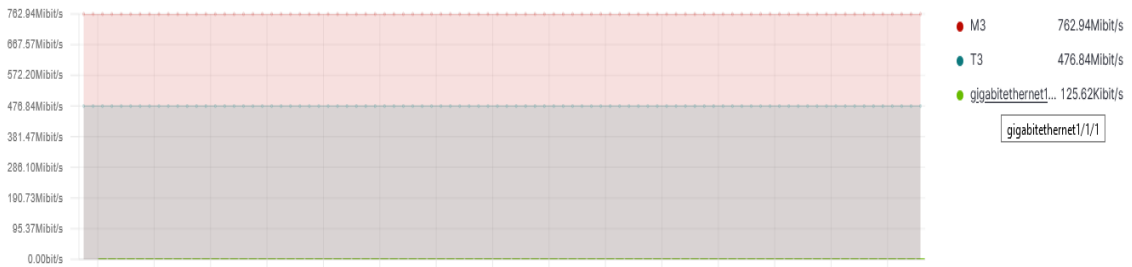

Figura 53. Tráfico entrante de la interfaz gigabit ethernet 1/1/1

A continuación, se presenta el tráfico saliente en la Figura 54, en la cual se aprecia que no supera los umbrales de *T4*=500Mbps y *M4*=800Mbps, el consumo de 1.28Kbps se observa en al lado de gigabit ethernet 1/1/1.

Figura 54. Tráfico saliente de la interfaz gigabit ethernet 1/1/1

- Resultados de la supervisión de los KPI (paquetes entrantes y salientes) del switch Cisco SG500-52 52-port Gigabit Stackable

La cantidad de paquetes entrantes y salientes se determinan como se muestran en la Figura 18. Para simplificar este proceso, se muestran las gráficas asociadas a una sola interfaz, sin embargo, la herramienta permite visualizar de manera independiente cada una de sus interfaces activas.

Debido a que cada protocolo red maneja diferentes tamaños en bit para cada uno de sus paquetes, el número máximo de paquetes que circulan por cada interfaz se define por medio de una aproximación. Analizando las gráficas, se puede identificar que el tráfico típico promedio no supera 400000 paquetes, por lo tanto, los umbrales serán *T5*=200000 y *M5*=320000. Analizando la gráfica 55 se observa que la cantidad de paquetes entrantes para la interfaz gi 1/1/31(gigabitethernet 1/1/31) no supera los umbrales *T5* y *M5* establecidos.

Se capturaron todos los paquetes que circulan por todas las interfaces de red física cada minuto

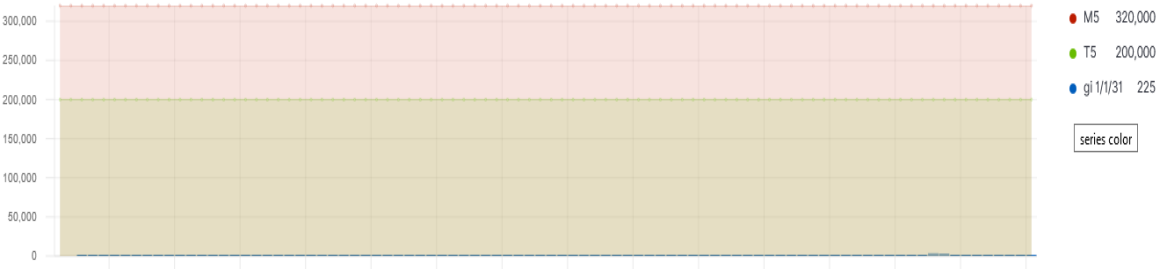

Figura 55. Cantidad de paquetes entrantes en la interfaz gigabit ethernet 1/1/31

Continuando con la supervisión de la cantidad de paquetes salientes en la interfaz gigabit ethernet 1/1/31, se repite proceso anterior para determinar los valores de referencia para *T6* y *M6*, los cuales son *T6*= 300000 y *M6*=480000. Como se observa en la Figura 56 la cantidad de paquetes no sobrepasa los valores umbrales de *T6* y *M6*.

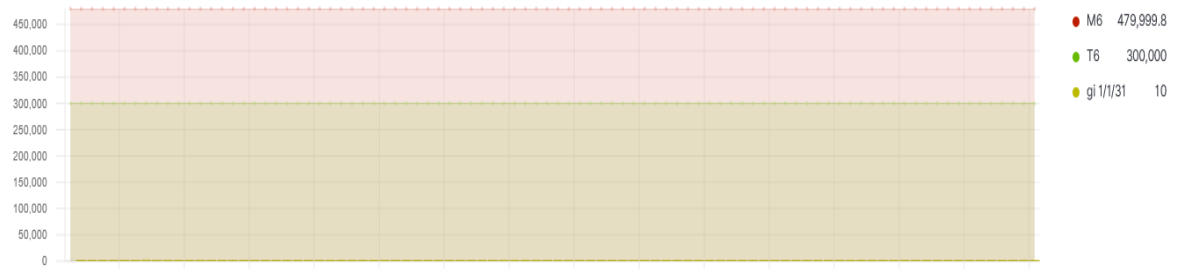

Figura 56. Cantidad de paquetes salientes en la interfaz gigabit ethernet 1/1/31

- Resultados de la supervisión de los KPI (paquetes descartados entrantes y salientes) del switch Cisco SG500-52 52-port Gigabit Stackable

Durante el tiempo que se realizaron las mediciones, se pudo comprobar que la cantidad de paquetes entrantes y salientes descartados es igual a 0, tal como se observa en la Figura 57. Por el resultado anterior no se crean valores de referencia para *T7*, *T8*, *M7* y *M8.*

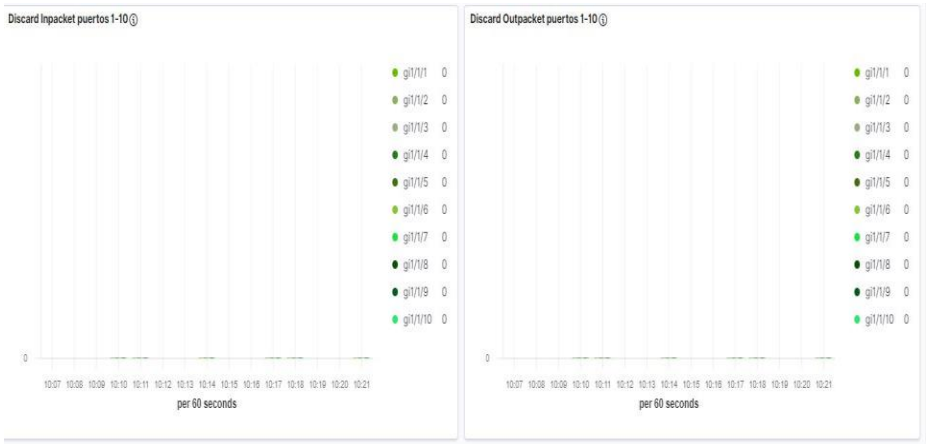

Figura 57. Paquetes perdidos entrantes y salientes de la interfaz gigabit ethernet 1/1/1 a la 1/1/10.

6. CAPÍTULO VI. Conclusiones y trabajos futuros

A continuación, se presentan las conclusiones y remediaciones obtenidas de la ejecución del trabajo de grado en modalidad práctica profesional: *Herramienta software para medición de desempeño de servicios sobre una infraestructura ti para la empresa KEYNETTIC S.A.S,* Además, se proponen trabajos futuros a partir del presente trabajo.

6.1 Conclusiones

- La herramienta *Elastic Stack* cuenta con todas la capacidades y funcionalidades necesarias para la medición del desempeño de los servicios TI.
- Se identificaron los KPI necesarios para la medición del desempeño del servicio de VoIP en una infraestructura de TI.
- La funcionalidad de *Machine Learning* dentro de *Elastic Stack,* permite identificar anomalías dentro de los datos y evitar así falsa alarma, y al mismo tiempo detectar datos inusuales que afecten de gravedad a los servicios TI.
- La herramienta *Elastic Stack* permite un alto grado configuración y adaptación según los requerimientos del usuario.
- Los agentes(*Beat*) consumen pocos recursos, evitando así impactar negativamente el desempeño de la red, convirtiéndolo en una opción viable para la gestión de una infraestructura TI.
- Las características de *Elastic Stack* permiten que el entorno de operación funcione más eficientemente y además permite acceder desde cualquier parte del mundo.
- La herramienta *Elastic Stack* resulta muy útil para la medición del desempeño de servicios TI, ya que permite el análisis de datos, creación de gráficas, alertas de toda la infraestructura en tiempo real.
- La experiencia de la práctica profesional me permitió aplicar conocimiento recibidos en algunas materias de énfasis y electivas cursadas en el programa.
- La práctica profesional me ayudo a fortalecer las habilidades técnicas y comunicativas, así como la adquisición de nuevos conocimientos de ingeniería.
- La práctica profesional me permitió enfrentar y abordar un problema y necesidad real de una empresa.
- Es importante y fundamental el diálogo y la realimentación continua con los asesores de la empresa, ya que permite tener un ritmo de trabajo adecuado para lograr apropiadamente los objetivos.

6.2 Recomendaciones

- Para trabajos relacionados con el uso de Logs donde se emplee *Logstash* con la entrada syslog, es importante cambiar el puerto que usa syslog por defecto el 514, ya que este es reservado por el sistema y puede que no se capture los datos y presente conflicto, es mejor usar un puerto en este rango 49152–65535.

6.3 Trabajos futuros

- Se propone para futuros proyectos la implementación del nuevo módulo de seguridad SIEM, incluido en la versión 7.8.1 de *Elastic Stack.*
- Se sugiere que para un análisis más profundo del desempeño de un servicio TI, se analicen características adicionales como: análisis de datos del consumo de disco duro, análisis de actualizaciones del sistema operativo.

BIBLIOGRAFÍA

[1] C. Cárdenas Mesa, “Propuesta de un modelo de gestión de servicio para la operación de ti de los operadores móviles de Colombia aplicando ITIL V3,” Tesis Doctoral, Universidad Santo Tomás, 2017.

[2] Organización para la Cooperación y el Desarrollo Económicos, “Perspectivas de la OCDE en Ciencia, Tecnología e Innovación en América Latina 2016”, OECD Publishing, Paris, 2016.

[3] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, “Boletín trimestral de las TIC cifra primer trimestre 2020,” MINTIC, Bogotá, 2020.

[4] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, “Estrategia integral para mejorar las condiciones de prestación de servicios fijos y móviles en Colombia,” MINTIC, Bogotá, 2020.

[5] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, “Plan TIC 2018-2022 El futuro digital es de todos,” MINTIC, Bogotá, 2020.

[6] M.Salcedo, “Herramientas informáticas basadas en las mejores prácticas para la Gestión de Servicios de TI de acuerdo con ITIL”. (Information Technology Infrastructure Library). Perspectivas, [S.l.], v. 13, n. 12, p. 3-11, jul. 2017. ISSN 1996-1952. Disponible en: http://revistas.uigv.edu.pe/index.php/perspectiva/article/view/201. [Acceso: 09 Nov. 2020]

[7] M. Carrasco, “Nivel de gestión de monitoreo y evaluación de tecnologías de información y la comunicación (tic), en la empresa Eleodoro Quiroga Ramos S.A.C. Sullana; 2018.”, Trabajo de titulación, Universidad Católica Los Ángeles, Chimbote, 2018.

[8] J. Vasconcelos Santillán, “Tecnologías de la información (2a. ed.)”, Grupo Editorial Patria, 2015.

[9] J. Gutiérrez, B. Guzmán, D. Chisco, “Guía de implementación de gestión de servicio de TI usando ITIL en las MIPYME”, Trabajo de titulación, Escuela Colombiana De Ingeniería Julio Garavito, Bogotá, 2017.

[10] A. López, L. Cieza, “Implementación de un Módulo de Seguimiento y Monitoreo de la Sección de Mesa de Ayuda del Área de TI en América Televisión en la ciudad de Lima - 2018”, Trabajo de titulación, Universidad Tecnológica de Perú, Lima, 2018.

[11] O. Meneses, “Catálogo de servicios de TI Versión 1.0”, Trabajo de titulación, ITSA Instituto tecnológico de Soledad Atlántico, Barranquilla, 2018.

[12] G. Duarte, “Arquitectura Propuesta para un Servicio Web Completo: Metodología de Desarrollo e Implementación”, Trabajo de titulación, Universidad Distrital Francisco José de Caldas, Bogotá, 2016.

[13] F. Hasny, *et al.*, “Predicting the Quality of Web Services based on User Stability”, IEEE International Conference on Services Computing (SCC), Beihang University, 2016.

[14] T.Mishra, G.Raj, “QoS implentation in Web Services Selection and Ranking using data Analysis”, Trabajo de titulación, Amity University, Uttar Pradesh, 2017.

[15] E. López, “Las ventajas y desventajas del internet en la sociedad”, CCD, vol. 2, n.º 1, pp. 35-45, ene. 2019.

[16] L. Boza, “Diseño e implementación del plan piloto de un sistema de comunicación VoIP usando tecnologías de código abierto”, Instituto Tecnológico De Costa Rica, Cartago, 2016.

[17] C. Gauloto, “Implementación del servicio de VoIP para los laboratorios de computación de la FICA”, Universidad de las Américas, Quito, 2018.

[18] M. Vinueza, “Estudio Detallado Del Uso Rtp/Rtcp Y Servicios De Qos Y Qoe En Internet Para La VOIP”, Escuela Superior Politécnica del Litoral, Guayaquil, 2015.

[19] J. Gonzales, “Marketing y Ecommerce. Parámetros de conducta del consumidor”, Universidad de la Laguna, Santa Cruz de Tenerife, 2020.

[20] M.Ramos, “Qué es el eCommerce: definición modelos y ventajas”. [En línea]. Disponible en: https://marketing4ecommerce.mx/que-es-el-ecommerce/. [Acceso: 15 Nov. 2020].

[21] A. Bloomenthal, “What Is Electronic Commerce” [En línea]. Disponible en: https://www.investopedia.com/terms/e/ecommerce.asp. [Acceso: 15 Nov. 2020].

[22] A. Sotelo, “Propuesta de implementación del protocolo netflow y la calidad de servicio para mejorar el rendimiento de la red lan en una sede de la SUNARP”, Universidad Nacional Tecnológica De Lima Sur, Lima, 2019.

[23] A. Valdez, *et al.*, “Calidad de servicio en redes de telecomunicaciones”, [En línea]. Disponible en: https://revistas.unne.edu.ar/index.php/eitt/article/view/2894. [Acceso: 15 Nov. 2020].

[24] IEEE Explore, “Not All Packets Are Equal, Part 2: The Impact of Network Packet Loss on Video Quality”, [En línea]. Disponible en: https://ieeexplore.ieee.org/document/4797940. [Acceso: Acceso: 15 Nov. 2020].

[25] Information Technology Infrastructure Library, Management Practices, “Measurement and reporting”, ITIL v4, 2020.

[26] A.Velia *et al.*, “Definición de Métricas de Calidad para Productos de Software”, XVIII Workshop de Investigadores en Ciencias de la Computación ,Entre Ríos, 2016.

[27] E. León, “Diseño y evaluación de un proceso de monitoreo de operaciones y control de métricas de servicios TI: Caso LABDC-UAA”, Trabajo de titulación, Universidad Autónoma de Aguas Calientes, Aguas Calientes, 2014.

[28] G. Hernández, Á. Martínez, R. Jiménez, F. Jiménez, “Métricas de productividad para equipo de trabajo de desarrollo ágil de software: una revisión sistemática”, TecnoLógicas, vol. 22, pp. 63-81, 2019. https://doi.org/10.22430/22565337.1510.

[29] F. Otarán, N. Perera, “Propuesta de una solución de monitoreo para sistemas del CeSPI”, Trabajo de titulación, Universidad Nacional de la Plata, La Plata, 2017.

[30] K. Espinal, E. Santos de la Cruz, “Métrica difusa para la evaluación del desempeño en la gestión por procesos”, Trabajo de titulación, Universidad Nacional Mayor de San Marcos, Lima, 2015.

[31] K. Buglioni, A. Contreras, “Propuesta de técnicas y herramientas para aplicar kpi de control y monitoreo en la implementación de proyectos TI.”, Trabajo de titulación, Pontificia Universidad Católica de Valparaíso, Valparaíso, 2018.

[32] G. Huerta Suárez, “Sistema de información para la gestión y extracción de KPI’s del área de tecnologías de información”, Trabajo de Grado, Instituto Tecnológico de Colima, Villa de Álvarez, 2016.

[33] A. Begoña, D. Alegre, “Gestión de Logs”, Tesis de Maestría, Universidad Internacional de La Rioja, La Rioja, 2016.

[34] M. Alpizar Santana, “Análisis de NAGIOS CORE como herramienta para el monitoreo de redes de datos”, Trabajo de titulación, Universidad Autónoma del Estado de México, Estado de México, 2017.

[35] N. Rodríguez, “Guía de buenas prácticas del proceso de monitoreo en un banco”, Especialización en proyectos informáticos, Universidad Distrital “Francisco José De Caldas”, Bogotá, 2019.

[36] J. Weller, “La pandemia del COVID-19 y su efecto en las tendencias de los mercados laborales,” Inicio, 03-Jul-2020. [En línea]. Disponible en: https://repositorio.cepal.org/handle/11362/45759. [Acceso: 25 Nov. 2020].

[37] M. Ortiz, A. Mori, “Influencia de la implementación de un sistema de monitoreo de infraestructura ti para gestionar las incidencias en la red lan del hospital regional de Cajamarca.”, Trabajo de titulación, Universidad Privada Antonio Guillermo Urrelo, Cajamarca, 2017.

[38] G. Junco, S. Rabelo, “Los recursos de red y su monitoreo”, Revista Cubana de Informática Médica 2018:10(1)76-83, 2018.

[39] F. Espinoza, “Monitoreo en tiempo real de DNS utilizando herramientas open source”, Trabajo de titulación, Universidad de Chile, Santiago de Chile, 2018.

[40] “Zabbix Documentation 5.2,” 2 What is Zabbix [Zabbix Documentation 5.2]. [En línea]. Disponible en: https://www.zabbix.com/documentation/current/manual/introduction/about. [Acceso: 25 Nov. 2020].

[41] About Nagios Core · Nagios Core Documentation. [En línea]. Disponible en: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html#whatis. [Acceso: 25 Nov. 2020].

[42] SolarWinds, “Solarwinds Network Performance Monitor,” 2017. [En línea]. Disponible en: https://www.solarwinds.com/-/media/solarwinds/swdc/pdf/npm/1702_npm_datasheet.ashx. [Acceso: 25 Nov. 2020].

[43] “PRTG Manual: Introduction: Monitoring with PRTG,” Paessler. [En línea]. Disponible en: https://www.paessler.com/manuals/prtg/introduction_monitoring_with_prtg. [Acceso: 25 Nov. 2020].

[44] Elasticsearch B.V., “What is Elasticsearch?” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html. [Acceso: 25 Nov. 2020].

[45] “Kibana-your window into Elastic” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/kibana/current/introduction.html. [Acceso: 27 Nov. 2020].

[46] Elasticsearch B.V., “Logstash Introduction,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/logstash/7.x/introduction.html. [Acceso: 27 Nov. 2020].

[47] Elasticsearch B.V., “What are Beats?,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html. [Acceso: 27 Nov. 2020].

[48] Elasticsearch B.V., “Metricbeat overview,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-overview.html. [Acceso: 27 Nov. 2020].

[49] Elasticsearch B.V., “Packetbeat overview,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/packetbeat/current/packetbeat-overview.html. [Acceso: 27 Nov. 2020].

[50] Elasticsearch B.V., “Winlogbeat Overviewedit,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html. [Acceso: 27 Nov. 2020].

[51] Elasticsearch B.V., “Auditbeat overviewedit,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/auditbeat/current/auditbeat-overview.html. [Acceso: 29 Nov. 2020].

[52] Elasticsearch B.V., “Heartbeat overviewedit,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/heartbeat/current/heartbeat-overview.html. [Acceso: 29 Nov. 2020].

[53] Elasticsearch B.V., “Filebeat overviewedit,” Elastic. [En línea]. Disponible en: https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html. [Acceso: 29 Nov. 2020].

[54] Windsor, G. and Windsor, G., 2021. A Guide to Project Initiation. [En línea] BrightWork.com. Disponible en: https://www.brightwork.com/blog/5-phases-of-a-project-initiating#.WjuCD1Wge70. [Acceso: 29 Nov. 2020].

[55] What is Project Management?. [En línea] Disponible en: https://www.pmi.org/about/learn-about-pmi/what-is-project-management [Acceso: 8 Dic. 2020].

[56] Ocampoale, V., 2021. Requerimientos Funcionales y No Funcionales, ejemplos y tips - Requeridos. [En línea] Requeridos. Disponible en:https://requeridos.com/requerimientos-funcionales-y-no-funcionales/ [Acceso: 8 Dic. 2020].

[57] Cloud.elastic.co. 2021. [En línea] Disponible en: https://cloud.elastic.co/pricing [Acceso: 8 Dic. 2020].

[58] Elastic.co. 2021. Precios de Elasticsearch oficial: Elastic Cloud, Elasticsearch gestionado. [En línea] Disponible en: https://www.elastic.co/es/pricing/ [Acceso: 8 Dic. 2020].

[59] support, P. and Switches, C., 2021. Cisco SG500-52 52-port Gigabit Stackable Managed Switch. [En línea] Cisco. Disponible en: https://www.cisco.com/c/en/us/support/switches/sg500-52-52-port-gigabit-stackable-managed-switch/model.html#~tab-downloads [Acceso: 8 Dic. 2020].

Anexo 1

1. Instalación y configuración de metricbeat

En esta sección se presenta los pasas para instalar y configurar *metricbeat,* los pasos se de instalación se ven en la Tabla 22.

#	Paso	Comando	Resultado/Paso alternativo/Observación	Figura/Tabla
1	Verifica si está instalado *curl*	*curl –version*	Pasar al paso 3 si está instalado Si no está instalado hacer el paso 2	
2	Instalar *curl*	*apt-get install curl*		
3	Descargar el agente metricbeat	*curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.8.1-amd64.deb*		
4	Descomprimir el archivo descargado	*sudo dpkg -i metricbeat-7.8.1-amd64.deb*	ok	
5	Acceder a la carpeta metricbeat para configuración	*/cd/etc/metricbeat*		
6	Editar el archivo metricbeat.yml	*/cd/etc/metricbeat/ nano metricbeat.yml*		Figura 58
7	Configurar los dos parámetros para la comunicación y envió de datos al servidor en la nube	***cloud.id: “”*** ***cloud.auth: “”*** **Nota:** Estos parámetros los da la herramienta cuando se crea el desarrollo de trabajo, el cloud.id es el identificador del desarrollo y el cloud.auth son las credenciales. Salir con ctl+x y dar aceptar para guardar cambios		Figura 59
8	Listar los módulos de metricbeat	*metricbeat modules list*	Verificar que el módulo system se encuentre en enable, si está en ese estado pasar al paso 10, sino realizar el paso 9	
9	Activar el módulo system	*metricbeat modules enable system*		
10	Modificar el archivo system.yml	*/cd/etc/metricbeat/modules/ nano system.yml* Salir con ctl+x y dar aceptar para guardar cambios		Figura 60
11	Verificar que las configuraciones estén correctas	*metricbeat test config*	Config ok	Figura 61

12	Instalar el metricbeat	*metricbeat setup*	Index setup finish	Figura 62
13	Activar el servicio de metricbeat	*systemctl metricbeat start*		Figura 63

Tabla 22. Instalación de metricbeat

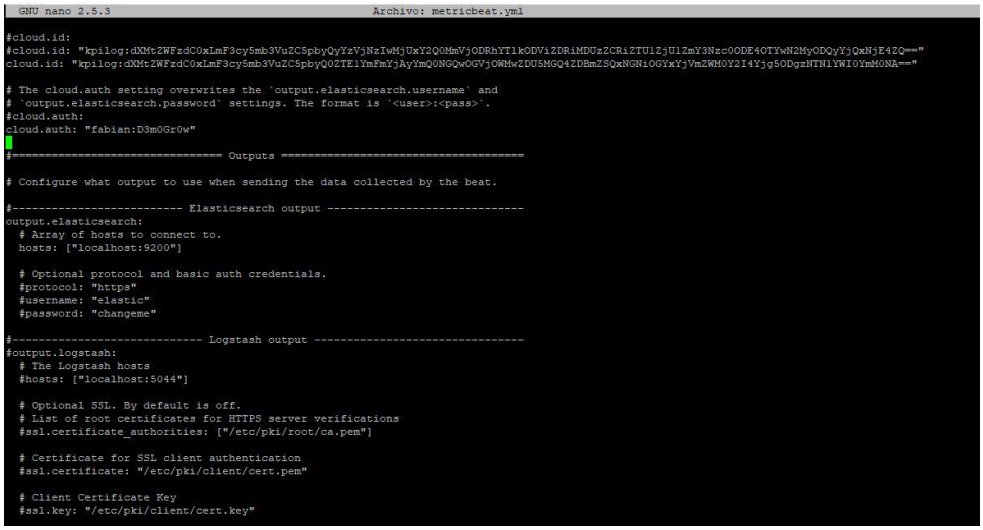

Figura 58. Archivo metricbeat.yml

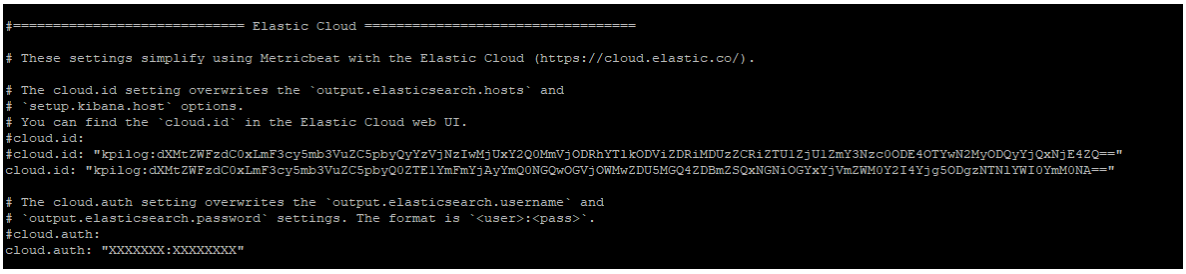

Figura 59. Parámetros para la comunicación y conexión con el servidor en la nube

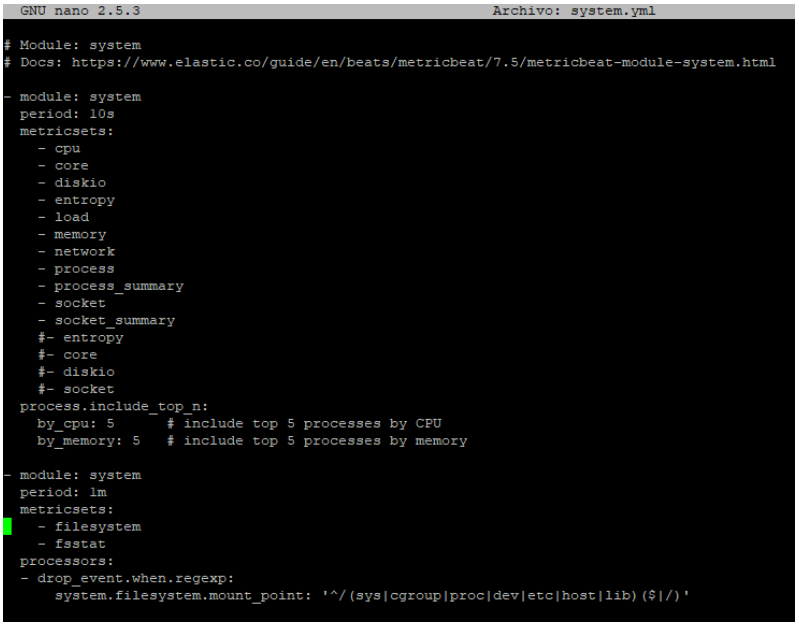

Figura 60. Archivo system.yml

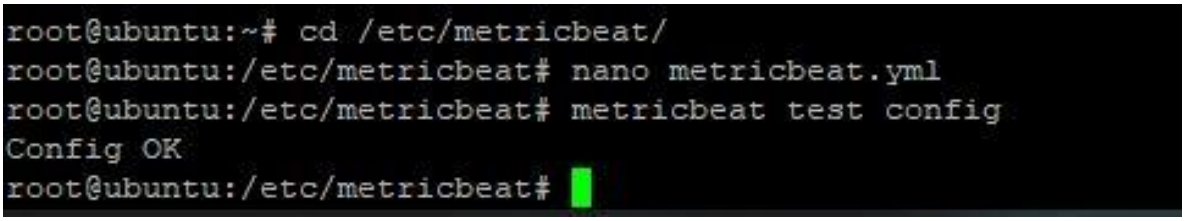

Figura 61. Verificación de la configuración y mensaje exitoso

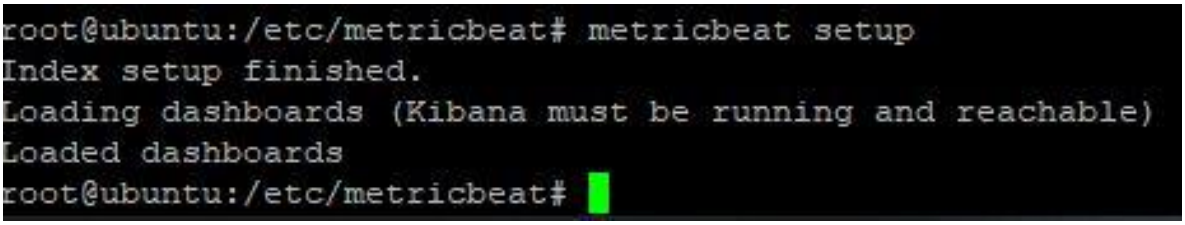

Figura 62. Instalación de metricbeat

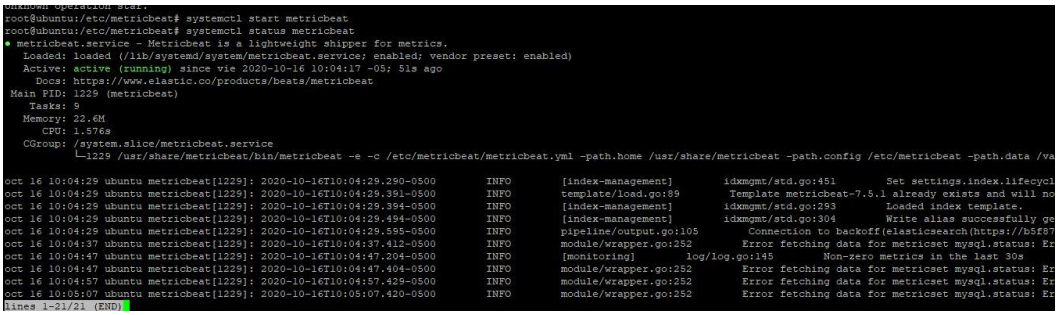

Figura 63. Activación del servicio metricbeat

2. Instalación y configuración de filebeat

En esta sección se presenta los pasos para instalar y configurar filebeat, los pasos se de instalación son mismo de la Tabla 23.

#	Paso	Comando	Resultado/Paso alternativo/Observación
1	Verifica si está instalado *curl*	*curl –version*	Pasar al paso 3 si está instalado Si no está instalado hacer el paso 2
2	Instalar *curl*	*apt-get install curl*	
3	Descargar el agente filebeat	*curl -L -O https://artifacts.elastic.co/downloads/beats/fielbeat/filebeat-7.8.1-amd64.deb*	
4	Descomprimir el archivo descargado	*sudo dpkg -i filebeat-7.8.1-amd64.deb*	ok
5	Acceder a la carpeta filebeat para configuración	*/cd/etc/filebeat*	
6	Editar el archivo filebeat.yml	*/cd/etc/filebeat/ nano filebeat.yml*	
7	Configurar los dos parámetros para la comunicación y envió de datos al servidor en la nube	***cloud.id: “”*** ***cloud.auth: “”*** **Nota:** Estos parámetros los da la herramienta cuando se crea el desarrollo de trabajo, el cloud.id es el identificador del desarrollo y el cloud.auth son las credenciales. Salir con ctl+x y dar aceptar para guardar cambios	
9	Configurar la entrada de file para que capture Logs	*filebeat.inputs:* *- type: log* *paths:* *- /var/log/messages* *- /var/log/*.log* Salir con ctl+x y dar aceptar para guardar cambios	
10	Verificar que las configuraciones estén correctas	*filebeat test config*	Config ok
12	Instalar el filebeat	*filebeat setup*	Index setup finish
13	Activar el servicio de filebeat	*systemctl filebeat start*	

Tabla 23. Configuración de filebeat

3. Configuración de parámetros SNMP en el Switch Cisco SG500-52 52-port Gigabit Stackable

La configuración en el Switch Cisco SG500-52 52-port Gigabit Stackable la realizó en el ingeniero a cargo de la supervisión de la práctica profesional. Primero se configuran los parámetros de la Tabla 24 para haya comunicación con el Switch, como se observa en la Figura 64. Después se incluyen las OID las cuales contienen los datos de interés como se muestra en la Figura 65.

Parámetro	Valor
Dirección IP	192.168.2.75
UDP Port	161
Community	public
Versión	SNMPv2

Tabla 24. Parámetros de configuración SNMP en el Switch Cisco SG500-52 52-port Gigabit Stackable

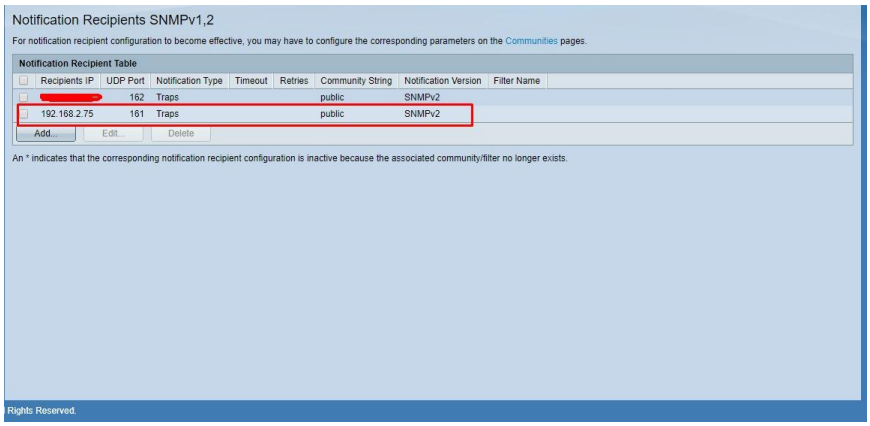

Figura 64. Parámetros de configuración SNMP dentro del Switch Cisco SG500-52 52-port Gigabit Stackable

Figura 65. OID incluidas en el Switch Cisco SG500-52 52-port Gigabit Stackable

4. Instalación y configuración de *Logstash*

La Tabla 25 se presenta los pasos para instalación y configuración de *Logstash* en el sistema operativo Debian para que puede enviar datos a *Elastic Cloud*.

#	Paso	Comando	Resultado/Paso alternativo/Observación
1	Verifica si está instalado *java*	*Java -version*	Pasar al paso 3 si está instalado Si no está instalado hacer el paso 2
2	Instalar *java*	*apt-get install default-jre*	
3	Descargar *Logstash*	*wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add* *sudo apt-get install apt-transport-https* *echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list*	
4	Instalar *Logstash*	*apt-get update* *sudo apt-get install logstash*	
5	Acceder a la carpeta *Logstash* para configuración	*/cd/etc/filebeat*	
6	Editar el archivo logstash.yml	*/cd/etc/logstash / nano logstash.yml*	
7	Configurar los dos parámetros para la comunicación y envió de datos al servidor en la nube	***cloud.id: “”*** ***cloud.auth: “”*** **Nota:** Estos parámetros los da la herramienta cuando se crea el desarrollo de trabajo, el cloud.id es el identificador del desarrollo y el cloud.auth son las credenciales. Salir con ctl+x y dar aceptar para guardar cambios	
8	Activar el servicio de logstash	*systemctl logstash start*	

Tabla 25. Configuración e instalación de *Logstash* para el sistema operativo Debian

5. Configuración de input SNMP dentro de *Logstash*

En la sección 7.4 se presentó la instalación de *Logstash*, ya instalado y funcionando se procede a configurar la entrada SNMP la cual permite capturar la información del switch Cisco SG500-52 52-port Gigabit Stackable en la Tabla 26 se muestran los pasos y la configuración terminada se aprecia en la Figura 66.

Pasos	Configuración
1	Se coloca el nombre del tipo de entrada, para este caso se coloca Input SNMP
2	Se asigna el valor a interval de 60, lo cual quiere decir que la información se solicita cada 60 segundos por SNMP Interval => 60

3	Se añaden las OID de interés el comando *get* es para solicitar 1 solo valor y el comando *Table* para solicitar datos de una tabla dentro de una OID
4	Se termina con los parámetros de a qué equipo se va a enviar los datos para este caso es: Host: dirección del equipo *Logstash* UDP/161 Communty => public Versión 2c

Tabla 26. Parámetros de configuración de la entrada SNMP en *Logstash*

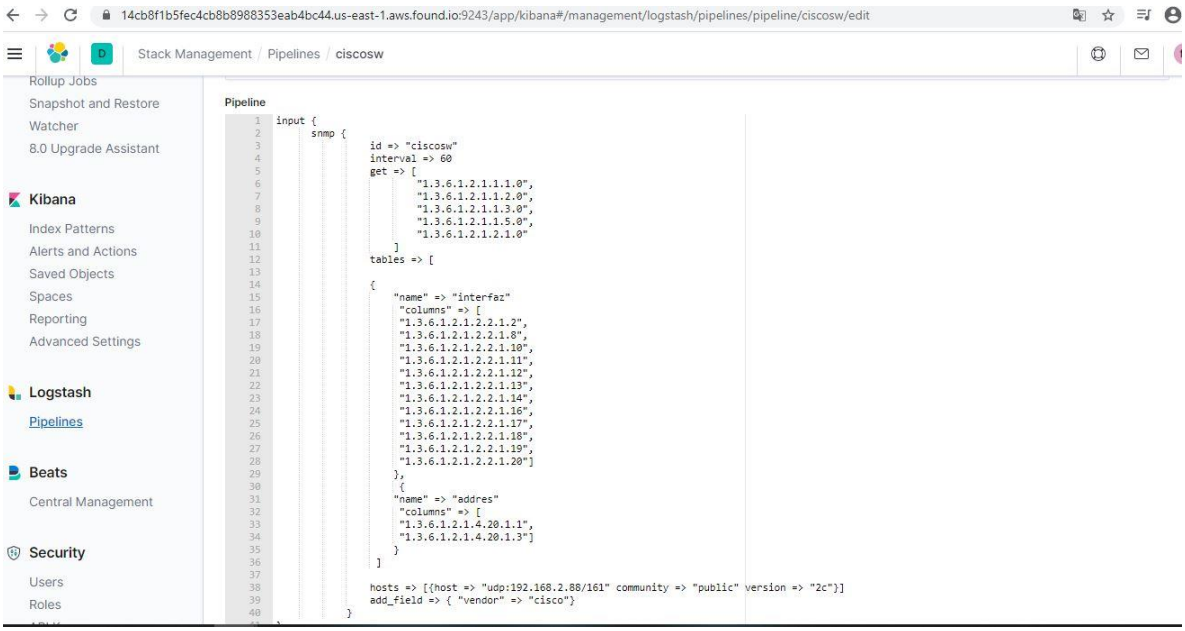

Figura 66. Configuración de la entrada SNMP para *Logstash*

6. Configuración de puertos para syslog en el Switch Cisco SG500-52 52-port Gigabit Stackable

La configuración del puerto para que el switch Cisco SG500-52 52-port Gigabit Stackable pueda enviar logs hacia *Logstash* es realizada por el ingeniero a cargo de la práctica profesional dentro de la empresa, en esta configuración se usa el puerto 62555, ya este no es un puerto privilegiado o está en uso por algún proceso del sistema, en Figura 67 se muestra la configuración dentro del switch.

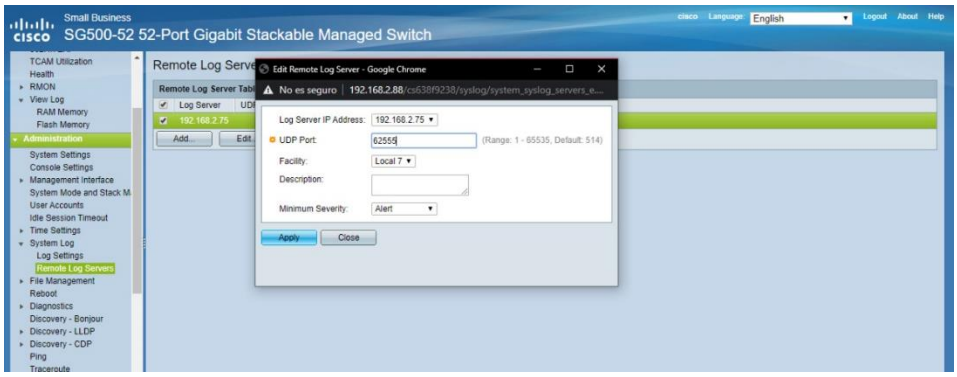

Figura 67. Parámetros de configuración del switch Cisco SG500-52 52-port Gigabit Stackable para enviar logs

7. Configuración de filtros logstash para procesar datos

En sección se presenta la configuración de los filtros que se usaron para procesar los datos que lo necesitaban. Los datos que se van a procesar son para 2 casos, uno para cambiar la extensión del campo que guarda la información y el otro para asignar cambiar el formato del dato de entero a string.

Para el primer caso de uso, se inicia creando el filtro con la palabra clave *filter*, dentro de este se coloca *mutate* para poder usar *rename*, este último es que permite cambiar el nombre del campo. En la línea código que se muestra a continuación, se cambia el nombre del campo "iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr" por el de campo "type", como se ve en la Figura 68.

"[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr]"=> "[interface][type]"

```
            hosts => [{host => "udp:192.168.2.88/161" community => "public" version => "2c"}]
            add_field => { "vendor" => "cisco"}
        }
}
filter {

  mutate {
    rename => { "iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0" => "[system][description]"
                "iso.org.dod.internet.mgmt.mib-2.system.sysName.0" => "[system][name]"
                "iso.org.dod.internet.mgmt.mib-2.system.sysObjectID.0" => "[system][objectid]"
                "iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0" => "[system][number][interfaces]"
                "iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.sysUpTimeInstance" => "sysuptime"
              }

        }
        ruby {
                code => "event.set('sysuptime', event.get('sysuptime').to_i / 360000 )"
        }
        mutate {
            rename => {
                "sysuptime" => "[system][uptime]"
            }
        }
        split {
                field => "interfaz"
        }
        mutate {
               rename => {
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr]" => "[interface][type]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus]" => "[interface][state]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets]" => "[interface][in][byte]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInUcastPkts]" => "[interface][in][uni][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInNUcastPkts]" => "[interface][in][non][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInDiscards]" => "[interface][in][discard][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInErrors]" => "[interface][in][error][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets]" => "[interface][out][byte]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutUcastPkts]" => "[interface][out][uni][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutNUcastPkts]" => "[interface][out][non][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutDiscards]" => "[interface][out][discard][pack]"
                          "[interfaz][iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutErrors]" => "[interface][out][error][pack]"
                          "[interfaz][index]" => "[interface][number]"
                        }
```

Figura 68. Filtro *rename* para cambiar nombre a los campos extensos por cortos

Para el segundo caso se desea cambiar el tipo de dato de entero a String. Lo primero que se hacer copiar el dato del campo "[interface][state]" a la variable “valor” por medio de *copy*, después la variable “valor” que contiene un valor entero se convierte a string con el uso de *convert*, como se muestra en la Figura 69.

```
    mutate {
      copy => { "[interface][state]"  => "valor" }
      }
      mutate {
                convert => { "valor" => "string" }
              }
  if "6" in [valor] {
     drop {  }
    }


    if "1" in [valor] {
      mutate {
              add_field => {
                  "state" => "up"
                          }
          }
      }
      else if "2" in [valor] {
       mutate {
              add_field => {
                  "state" => "down"
              }
          }
      }
```

Figura 69. Proceso para cambio de tipo de dato de entero a string

8. Creación de visualizaciones

En esta sección se presenta los pasos para crear las visualizaciones hechas con la información recolectada con la herramienta *Elastic Stack*.

Visualización que hacen uso de la plantilla Gauge

Para mostrar datos de las métricas de CPU y memoria RAM se emplea *Gauge*. A continuación, en la Tabla 27, se enuncian y describen los pasos para la creación de esta visualización.

#	Paso/ acción	Comentario	Figura
1	Dirigirse a la **Kibana/Visualice**	Presionar en el botón **create visualization**	Figura 70
2	Seleccionar TSVB		Figura 71
3	Seleccionar Gauge (dentro de TVSB)	El panel de la visualización TSVB tiene cuatro opciones time series, metric, top N, markdwon, table (en la Tabla 15 se especifican características)	Figura 72 Figura 73
4	Seleccionar y configurar **Data**	Seleccionar average (promedio)	Figura 74
5	Cambiar el formato de los datos	Seleccionar Percent (muestra el valor en porcentaje)	Figura 75
6	Añadir rango de niveles por medio de colores	En la sección de panel options, abajo en ***Style*** Se colocan los valores para que muestre un color según sea el valor medido, el color indica si está en nivel de criticidad, el color verde se usa para valores normales y el rojo para valores críticos .	Figura 76

Tabla 27. Creación de visualización TSVB para mostrar la información de CPU del servidor de VoIP

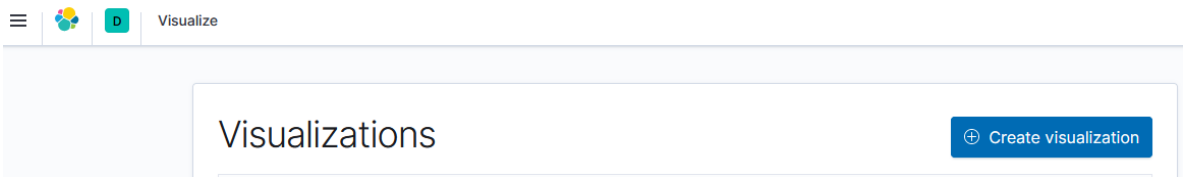

Figura 70. Creación de visualizaciones dentro de *Kibana*

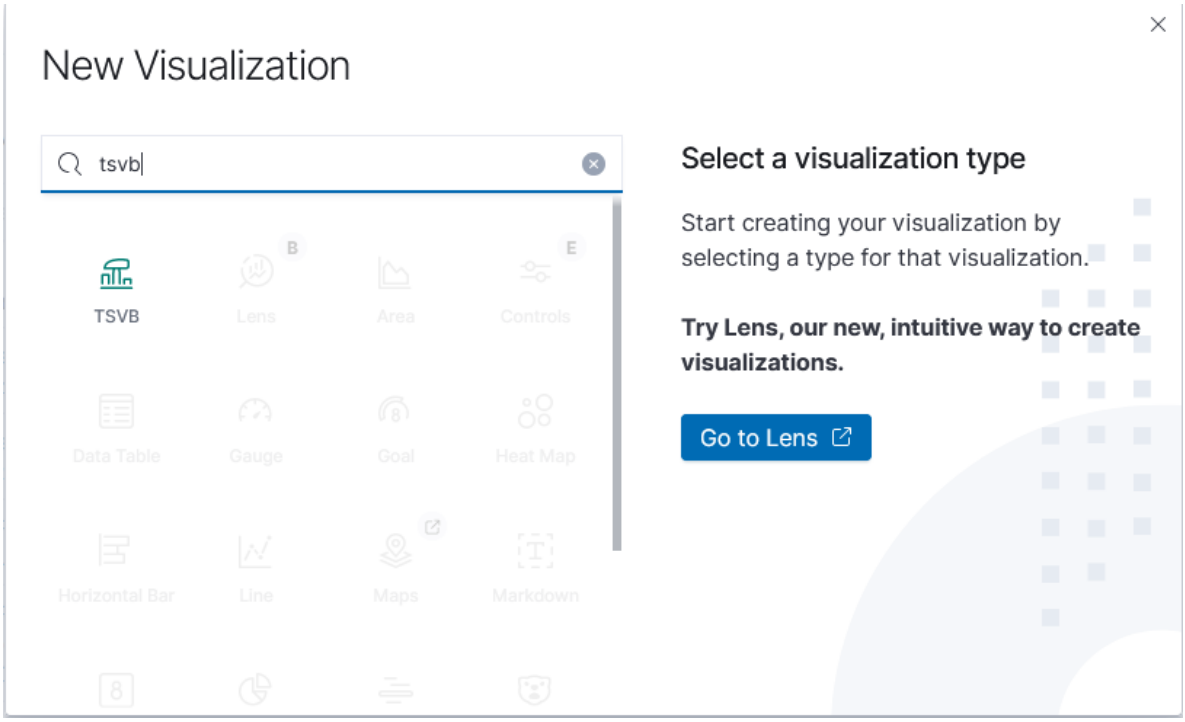

Figura 71. Visualización TVSB

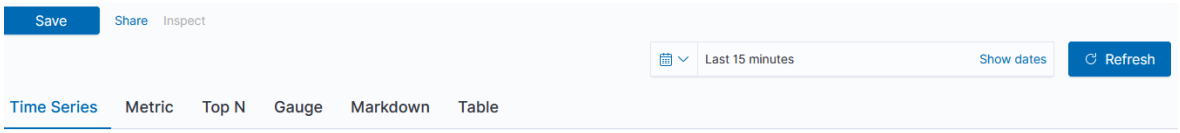

Figura 72. Panel de opción de TSVB

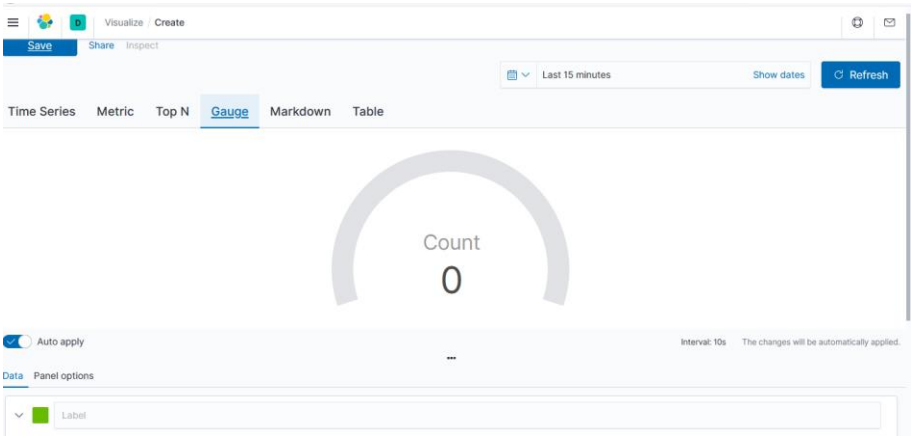

Figura 73. Configuración de Data para mostrar la información

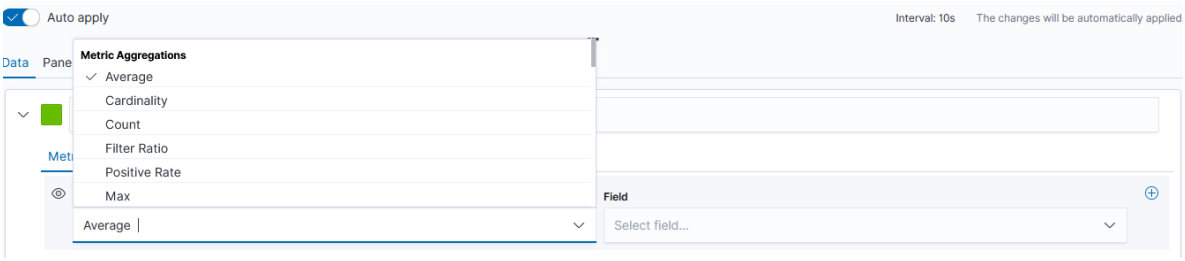

Figura 74. Selección de la agregación de la métrica

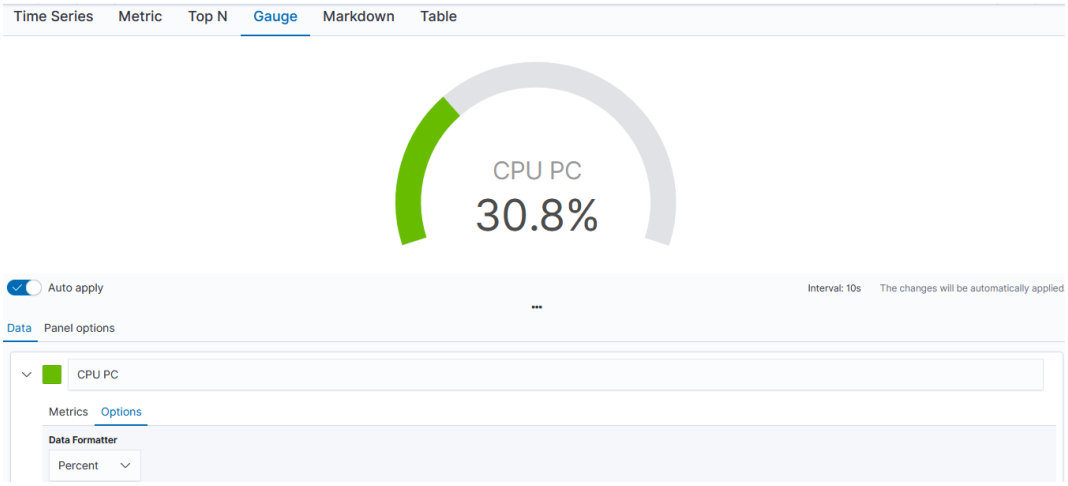

Figura 75. Visualización en tiempo real del consumo de CPU

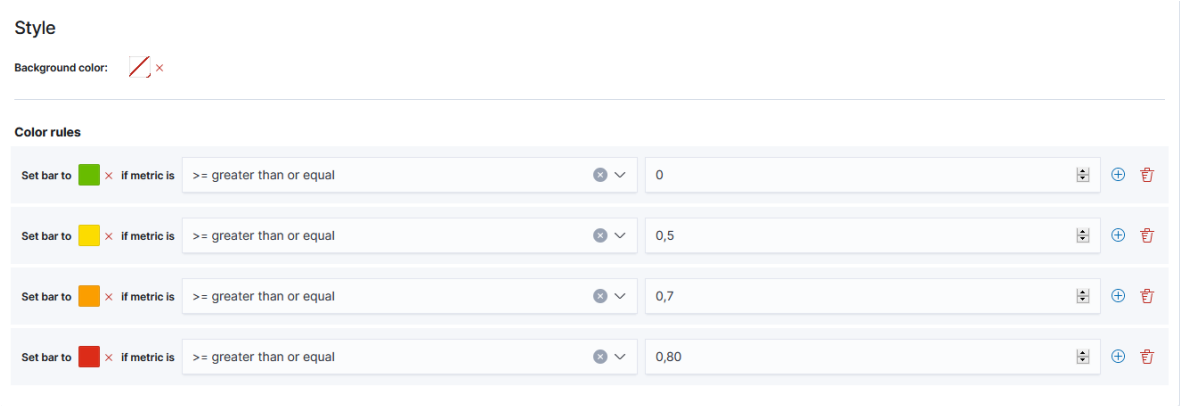

Figura 76. Configuración de lo nivel de criticidad por medio de colores

Visualización de información de memoria RAM

Para mostrar datos de las métricas de memoria RAM, se selecciona la visualización *Goal*, teniendo en cuenta las características. A continuación, se enuncian y describen los pasos para la creación de esta visualización en la Tabla 28.

#	Paso/ acción	Comentario	Figura
1	Dirigirse a la **Kibana/Visualice**	Presionar en el botón **create visualization**	
2	Seleccionar Goal		Figura 77
3	Seleccionar y configurar **Option**	Configurar los rangos para asignar colores según sea el nivel Verde indica rango valores bajo. Amarillo indica rango valores medio. Rojo indica rango valores alto.	Figura 78

Tabla 28. Creación de visualización Gauge para mostrar la información de Memoria RAM expresada en porcentaje del servidor de VoIP

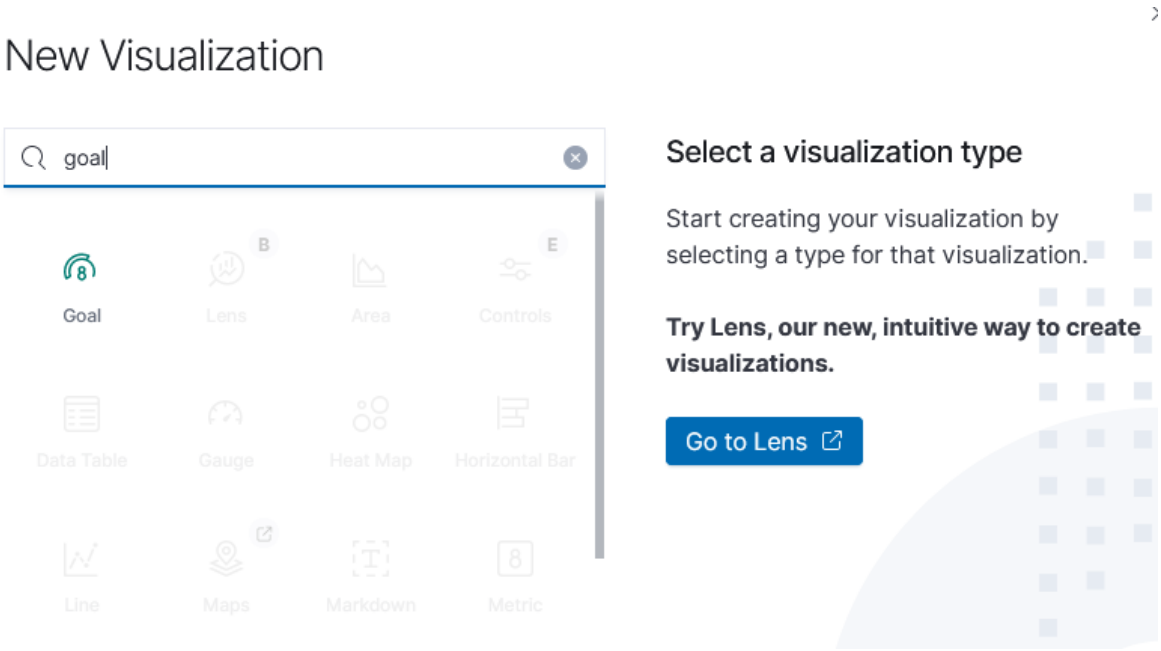

Figura 77. Selección de la visualización Goal

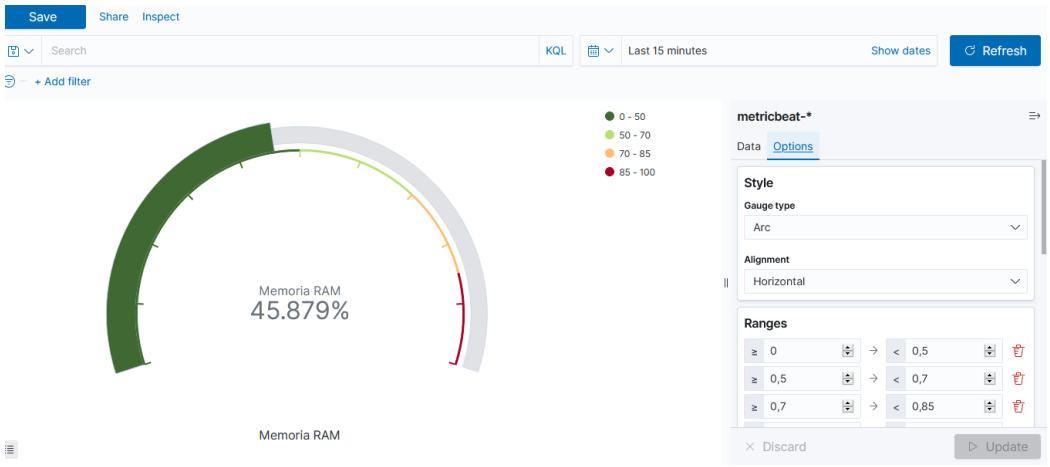

Figura 78. Visualización en tiempo real del consumo de memoria RAM del servidor VoIP

Visualización de la cantidad procesos activos

Para mostrar datos de cantidad de procesos activos, se selecciona la visualización *Metric* ya que esta permite mostrar un único valor. En la Tabla 29 se enuncian y describen los pasos para la creación de esta visualización.

#	Paso/ acción	Comentario	Figura
1	Dirigirse a la **Kibana/Visualice**	Presionar en el botón **create visualization**	Figura 79
2	Seleccionar Metric		Figura 80

Tabla 29. Pasos para la creación de la visualización del registro de la cantidad de procesos activos en el servidor de VoIP

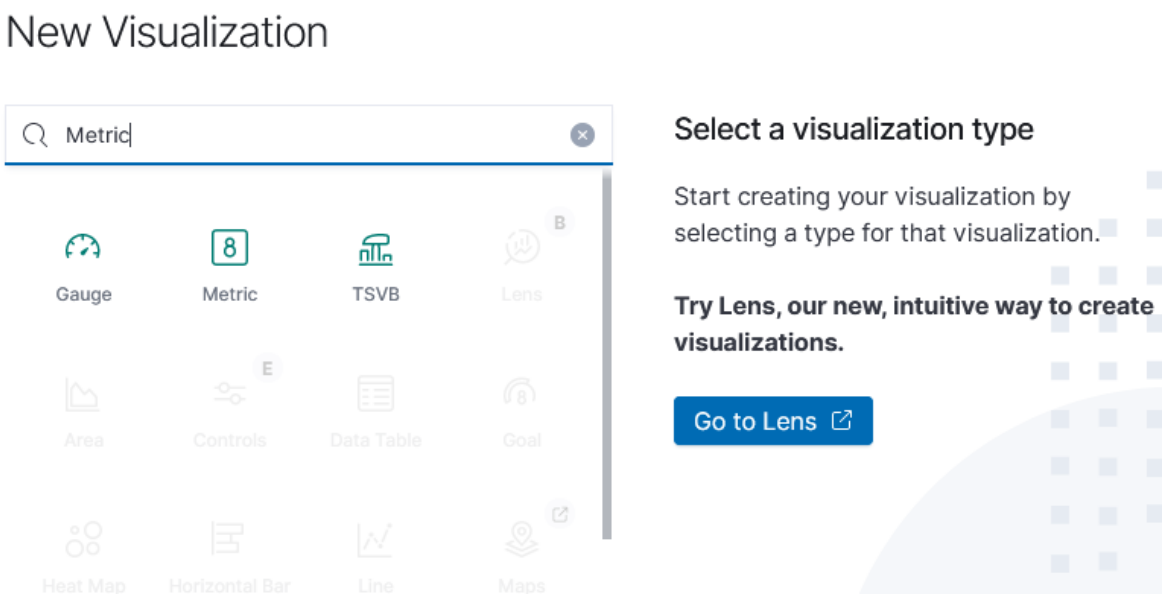

Figura 79. Selección de la visualización Metric para cantidad de procesos activos

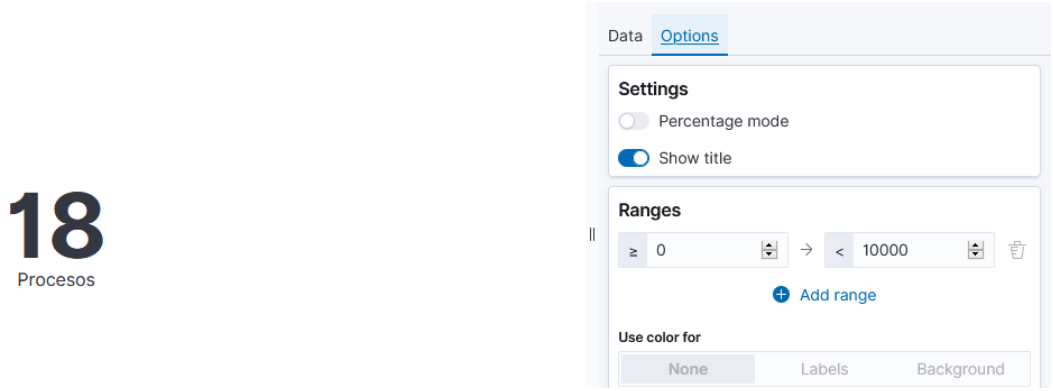

Figura 80. Visualización de los procesos activos en el servidor de VoIP

Visualización de datos de consumo de memoria RAM y CPU de los procesos activos

Para mostrar datos de las métricas de consumo de memoria RAM y CPU por los procesos ejecutados dentro del servidor de VoIP, se selecciona la visualización TSVB, teniendo en cuenta las características y la forma de presentar la información. En la Tabla 30 se enuncian y describen los pasos para la creación de esta visualización.

#	Paso/ acción	Comentario	Figura
1	Dirigirse a la **Kibana/Visualice**	Presionar en el botón **create visualization**	
2	Seleccionar TSVB		
3	Seleccionar Top N (dentro de TVSB)	El panel de la visualización TSVB tiene cuatro opciones time series, metric, top N, markdwon, table	Figura 81
4	Seleccionar y configurar **Data**	Seleccionar average (promedio)	
5	Cambiar el formato de los datos	Seleccionar Percent (muestra el valor en porcentaje)	
6	Se agrupan los datos por procesos		Figura 82

Tabla 30. Pasos crear la visualización del consumo de memoria RAM y CPU por proceso

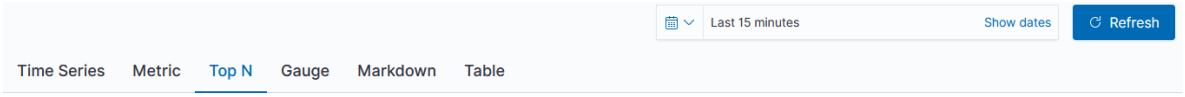

Figura 81. Sección Top N dentro de la visualización TSVB

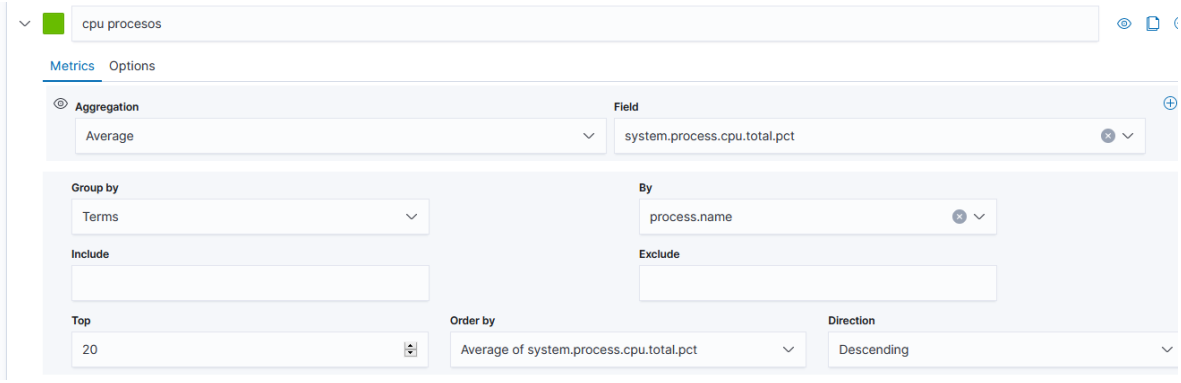

Figura 82. Parámetros de configuración para mostrar el consumo de CPU por proceso activo

Visualización de tráfico entrante y saliente del del switch Cisco SG500-52 52-port Gigabit Stackable

Esta visualización se realiza por medio de TVSB y el uso de una agregación llamada ***serial differencing*** [1], esta permite restar valores de sí mismo en periodos de tiempo, esta función es de gran utilidad ya que los valores que se obtienen de switch Cisco SG500-52 52-port Gigabit Stackable para el tráfico entrante y saliente son valores de una variable contador, esta variable cuenta e incrementa el valor, pero no da el valor instantáneo. Este procedimiento se usa para hacer la visualización de tráfico saliente, cantidad de paquetes salientes, cantidad de paquetes entrantes descartados, cantidad de paquetes salientes descartados. Los pasos para realizar se presentan en la Tabla 31 y la visualización terminada se aprecia en la Figura 85.

#	Paso/ acción	Comentario	Figura
1	Dirigirse a la **Kibana/Visualice**	Presionar en el botón **create visualization**	
2	Seleccionar TSVB		
3	Seleccionar Time series (dentro de TVSB)	El panel de la visualización TSVB tiene cuatro opciones time series, metric, top N, markdwon, table.	
4	Seleccionar y configurar **Data**		
5	Cambiar el formato de los datos	Seleccionar Custom y el formato es bitb para que se pueda mostrar en bit.	Figura 83
6	Incluir fórmula para adecuar los datos	Como los datos son capturados en octetos 1 octeto=Byte=8bit La fórmula implementar es: (Octetosin1*8)/60 Se multiplica por 8 para pasarlo a bit y se divide en 60 porque la muestra se toma cada minuto, cada 60 segundos de esta manera obtenemos bps, bit/seg	Figura 84

Tabla 31. Pasos para crear la visualización de tráfico entrante y saliente del switch Cisco SG500-52 52-port Gigabit Stackable

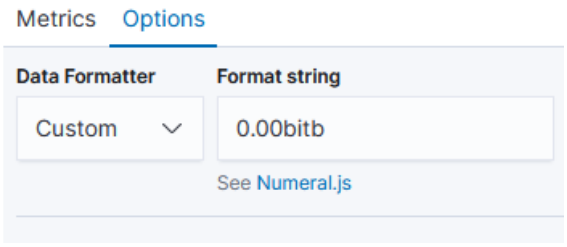

Figura 83. Cambio de formato de datos para presentarlo en bit

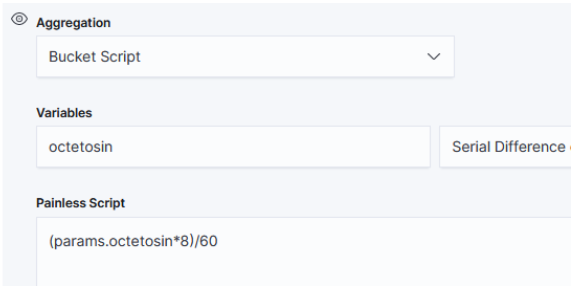

Figura 84. Implementación de la fórmula para calcular bps dentro de la visualización

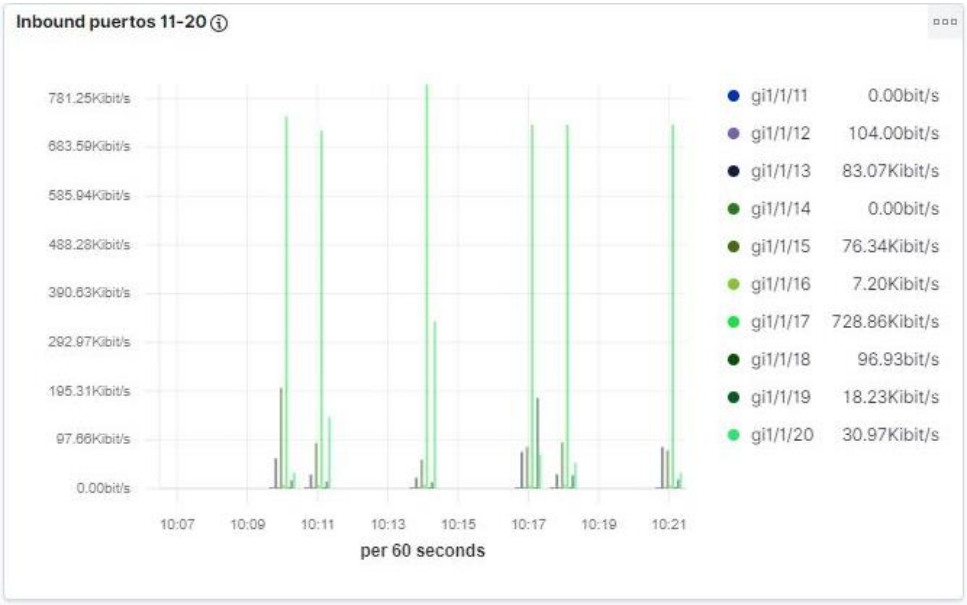

Figura 85. Visualización de tráfico entrante de las interfaces físicas del switch Cisco SG500-52 52-port Gigabit Stackable

9. Creación de cuenta Slack

Slack es el conector que se creó dentro de las alertas para que se envíen las notificaciones allí. Para usar Slack hay que crear una cuenta con un correo personal o de trabajo en la siguiente dirección electrónica https://slack.com/get-started#/create, terminada la creación de la cuenta, se crea el nombre del espacio de trabajo el cual es **demomonitor**, el nombre del espacio de trabajo es el parámetro que se coloca en el conector de la alarma dentro de *Elasticsearch*¸ para que este sepa a donde enviar la advertencia cuando se active la alarma. Finalmente, la información de la alarma aparece en el canal que se creó dentro de **demomonitor** con el nombre **monitoreo** como se aprecia en la Figura 86.

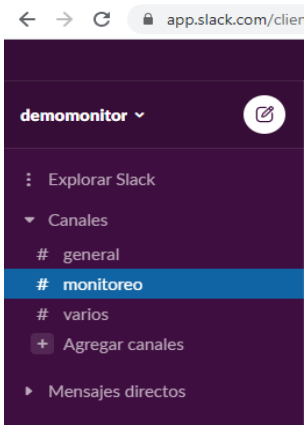

Figura 86. Espacio de trabajo en Slack donde llegan las alertas de *Elasticsearch*

Bibliografía

[1] Elastic.co. 2021. Serial differencing aggregation | Elasticsearch Guide [7.12] | Elastic. [En línea] Disponible en:ttps://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations-pipeline-serialdiff-aggregation.html [Acceso: 15 Mar 2021].